



---

**SMART 2007/0005**

**Survey and Analysis of EU ICT  
Security Industry and Market  
for Products and Services**

**D.7.4 Final Study Report  
The Evidence Base: Critical  
Issues Analysis**

---

IDC Government Insights

April 2009



**SMART 2007/0005**

**Survey and Analysis of EU ICT Security Industry and Market for Products and Services**

**D.7.4 Final Study Report  
The Evidence Base: Critical Issues Analysis**

---

The opinions expressed in this Report are those of the authors and do not necessarily reflect the views of the European Commission.

Author(s)	IDC European Competitiveness and Innovation Expertise Centre – Government Insights
Deliverable	D.7.4 Draft Final Study Report: The Evidence Base: Critical Issues Analysis
Date of delivery	April 30, 2009
Version	1.0
Addressee officers	Gerard Galler European Commission Information Society & Media DG Unit A3: Internet; Network and Information Security Office BU33 05/087, 33 Avenue Beaulieu, B-1160 Bruxelles Tel: +32 2 299 93 55, e-mail: gerard.galler@ec.europa.eu
Contract ref.	Contract Nr 30-CE-0150192/00-00

## TABLE OF CONTENTS

P

<b>1. Introduction</b>	<b>1</b>
<b>2. Mapping the Main Stakeholders of the NIS Market</b>	<b>2</b>
National/Regional Governments .....	3
University and Research Institutions.....	9
Standardization and Certification Bodies .....	9
Lawyer Firms and Insurance Companies .....	10
Professional and End User Associations .....	11
<b>3. Main Drivers and Barriers of the NIS Market: Stakeholders Opinions</b>	<b>12</b>
Profile of Stakeholders Interviews.....	12
Opinions on Main Drivers of Demand.....	13
Opinions on the Main Challenges for the Market Development.....	16
Opinions on NIS Market Supply-Demand Match and Maturity.....	18
<b>4 Opinions on the Regulatory Framework of the NIS Market</b>	<b>20</b>
The emerging IT security Insurance Services Market.....	22
The case of Estonia and the emerging threats of cyber-attacks .....	23
Main Conclusions on Stakeholders Opinions .....	26

## LIST OF TABLES

	P
1 Main Stakeholder Categories and Roles in the NIS Market .....	3
2 List of Stakeholders Interviews.....	12
3 Stakeholders Opinions on NIS Market Main Drivers and Barriers.....	15
4 Stakeholders Opinions on NIS Markets Development Main Challenges.....	17
5 Stakeholder Opinions on NIS Markets Maturity and Match Demand-Supply .....	19
6 Stakeholder Opinions on Cooperation at the EU level .....	20
7 Stakeholder Opinions on Insurance Services for the NIS market .....	23

## 1. INTRODUCTION

The focus of this study is the Network and Information Security Market in the EU27. This report is part 4 of the Final Study Report (**Deliverable 7.4: The Evidence Base: Critical Issues Analysis**) produced by IDC EMEA for the study “Survey and Analysis of the EU ICT Security Industry and Market for Products and Services” on behalf of the European Commission, DG Information Society and Media.

This report presents the detailed results of the qualitative analysis of the main critical issues for the development of the NIS market, carried out on the basis of desk research and interviews with a selected sample of stakeholders. The goal of this research was to provide depth and understanding to the NIS market scenario.

This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

The other components of the Draft Final Study Report are:

- **D.7.1 - The EU NIS Market: Scenario, Trends and Challenges**, which presents the overall NIS market scenario, the main conclusions and recommendations of the study, and the set of indicators proposed to monitor the market. This report is addressed to policy makers and main stakeholders.
- **D.7.2 – The Evidence Base: Demand Analysis**, which presents the detailed results of the business and consumer demand analysis. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.
- **D.7.3 - The Evidence Base: Supply Analysis**, which presents the detailed results of the supply analysis. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

The authors of the study are a multidisciplinary group of experts from multiple units of IDC EMEA and MIP Politecnico. The project manager is Gabriella Cattaneo, Director of IDC EMEA Competitiveness and Innovation Expertise Centre, part of IDC Government Insights. Eric Damage, IDC Security Research Manager, Giuliana Folco, VP of IDC EMEA Industry Solutions Expertise Centre, and IDC CEMA (Central and Eastern Europe, Middle East and Africa) participate in the study team.

## **2. MAPPING THE MAIN STAKEHOLDERS OF THE NIS MARKET**

The interaction between suppliers and users, intermediated by distribution channels, is at the core of the Network and Information Security (NIS) market. But there are many other categories of stakeholders influencing the development of the NIS market. They are identified in the following table and classified on the basis of their main role in the NIS market.

The study identified the following main stakeholder categories:

- Stakeholders engaged in security policy development and implementation are arguably the most important group, because of their power to shape the market scenario and the regulations to be respected by suppliers and users. This group includes European institutions, Federal/National/Regional Governments, and various NIS public bodies.
- Stakeholders active in Security Risks Management, that is all the public and private organizations supervising the management of security breaches, organizing and coordinating counteractions and protection against main security threats, at the national or local level, for specific industries (for example banks). Some of them are organized by main security vendors for their clients only.
- Stakeholders engaged in technical management and innovation development in the NIS market include Standardization and Certification bodies, and also University and Research Centres, who are also active in education and training. These stakeholders provide critical building blocks for the development of the NIS market, that is innovative technical solutions and specialized human resources. These stakeholders interact closely and often cooperate with security vendors, who are also active in technical innovation and skills development, but naturally in the context of their own business strategies.
- Stakeholders providing specialized support services to the NIS market include business consultants, lawyer firms and insurance companies. The diffusion of the Internet is leading to the emergence of a niche market for these specialized services.
- Stakeholders active in the social dialogue on IT security issues, including industry or professional associations representing the interests of business users, Internet users associations representing the interests of consumers for issues such as privacy protection and children protection, and Internet professional associations involved with IPR in cyberspace issues.

The following paragraphs describe more in detail their activities and interactions.

**TABLE 1**

## Main Stakeholder Categories and Roles in the NIS Market

Category of Stakeholder	Description	Main Role in the NIS scenario
European Institutions	European Commission ENISA (European Agency for Network and Information Security)	Security Policy Development
National/ Federal Government Bodies	Ministry of Communications, NRA, Ministry of Interior, Ministry of Defense	Security Policy Development
Public NIS Bodies	National Agencies for Security, or Ministry Departments with responsibility for Security	Security Policy Implementation
CERTs (Computer emergency Response Team), CIIP (Critical Information Infrastructures Protection) bodies	Public and private organizations supervising security breaches, and managing the protection of critical information infrastructures (including utilities, telecom operators, railways and airport management)	Security Risks Management
Standardization and certification bodies	ISO, ETSI, ICTSB, IETF	Technical Management and Innovation
University and Research	Main universities IT departments, private and public IT security research centres	Technical Management, innovation, education and training
Professional services	Lawyer firms and insurance companies	Expert support services to associations and end users
Professional and End user associations	Associations of security professionals (CLUSIF) and/or Industry groups (e.g. EICTA) or Consumers associations for privacy protection or fighting cybercrime	Social Dialogue

Source: Government Insights, 2008

**National/Regional Governments**

National (and to a lesser extent, Regional) Governments are among the most important actors in the NIS market scenario, because of their different roles: on the one hand they develop and/or implement regulation and policies on a range of critical issues, on the other hand public organizations are important IT security users, who are expected to act as good practice examples. In this paragraph we consider mainly their role as market influencers rather than users (as this is examined in the Demand analysis report).

The regulatory framework governing the NIS market covers a wide range of issues, which can be summarized in the following main policy areas:

- Protection of Privacy of personal and sensible information and data on electronic devices and networks;
- Electronic Communications Regulatory Framework, addressing the main suppliers and service providers of ICT industries, including for example data protection and data retention requirements for telecommunication service providers;
- Provisions for the protection of Critical Information Infrastructures;
- Regulation for the prevention of financial losses/frauds and Risk management in the Financial sector
- Electronic Identity and Authentication regulation (for example the new Electronic Passport, e-passport, equipped with an integrated circuit for biometric identification);
- Laws against Cyber crime, Cyber-terrorism, Child Pornography on the Internet, and similar crimes.

Most of these regulation areas are characterized by a double layer, composed by strategic directives or guidelines at the European Union level, accompanied by national/federal government laws or regulation at the Member States level (with implementation and some regulation which may done at the regional/state government). The role of EU regulation has been more relevant in some fields (typically Data protection and Electronic Communications), while Security policies as such remain in the national governments domain, even if intergovernmental cooperation has been growing rapidly.

In addition, the NIS market may be influenced by:

- Research and Innovation policies regarding ICT technological innovation, higher education institutions for ICT, investments in R&D for NIS technologies and the ICT industry;
- Industry policies for the ICT industry and/or SMEs (as security users or as ICT producers).

This summary proves how many different government actors are involved at different levels with the NIS market. While institutions and responsibilities vary substantially, generally the most important government actors defining the strategic policies for NIS issues are:

- The Ministry of Communications, overseeing communication networks policies (sometimes it is a department of a larger Ministry), sometimes Critical Information Infrastructures protection;
- The National Regulatory Agency for Electronic Communications;
- The National Office for Data Protection

- The Ministry of Interior overseeing national security, electronic identity, cyber crime policies;
- The Ministry for Public Administration (or reform of public administration, or eGovernment, whatever) overseeing policies of NIS use within the government itself;
- The Ministry of Defense may share with the Ministry of Interior the definition of policies against cyber-terrorism and is normally a very important customer of specialized NIS products and services.

These Government actors operate at the strategic policy level and rarely interact directly with individual NIS market suppliers or users, rather they may consult or be contacted by industry or lobby associations. They interact instead with the EC level actors for policies development. They are often supported by operative agencies more focused on the actual implementation of security policies, monitoring of NIS threats and attacks, organizing and coordinating counter-measures, promoting awareness and education campaigns. They are described in the following paragraph.

#### ***Public Network and Information security bodies***

Public Network and Information Security bodies are typically created to implement National Programmes for IT security, or are born as the IT security arm of some Ministry (more often the Ministry of Interior or Ministry of Defense). Their primary goal is to promote IT security at the national level, providing advice and recommendations, analysing the national security situation and defining plans and other initiatives (as building relationships and cooperation between different players).

Typically they have very broad responsibilities, especially in the case of large organizations (such as BSI in Germany, or the DCSSI in France). Their main tasks concern information gathering for important IT security issues, consultancy (developing scientific and technical expertise), and specialized input to main government policies in the area. Many of them have the responsibility to approve, guarantee and certificate the Security of National information systems, participate to the development of IT security applications and products for the public sector or for public interest projects. Some of them are also in charge of national strategies in the area of CIP and CIIP.

These Public Bodies are typically active in national and international networking activities for information sharing and risk management with their counterparts, or with other, less specialized, public bodies in their countries.

These National security bodies provide services to the users and manufacturers of information technology products. Their main users are usually other public agencies at the national and local level (these bodies often lead the development of NIS measures for public networks and information infrastructures). But they may also provide services to the private sector (more often certification).

According to the most recent analysis by ENISA, EU countries with the most advanced and mature NIS markets (Northern Europe, France and Germany for example) tend to concentrate these activities in one single main Agency (while in many MS these competencies may be divided among several different public agencies).

The most important examples are:

**Denmark:** the National IT and Telecom Agency. Area of responsibility: general IT security, e.g. consultancy to citizens and governments, Information and awareness creating activities, Protection of the IT and TLC infrastructures, Standardization of IT security, IT and telecom emergency preparedness, Electronic Signatures..

**France:** Central directorate for Information Systems Security (DCSSI). Area of responsibility: Regulation, Operation, Science and Technology in information systems security.

**Germany:** Bundesamt für Sicherheit in der Informationstechnik (BSI). Area of responsibility: BSI is the central IT security service provider for the German federal government. Furthermore it advises manufacturers, distributors and users of information technology. BSI provides services for instance in the fields of: IT security management, Internet security, Security in mobile devices, Network security, Certification of products.

**Sweden:** Swedish Emergency Management Agency (SEMA). Area of responsibility: SEMA has overall governmental responsibility for information assurance in Sweden. The agency follows the development in the field of information security (in terms of threats, vulnerabilities protective measures and risks) and presents an annual assessment to the Government. SEMA also works in a preventive capacity with IT security issues, conducting IT security analyses and giving advice and recommendations. The agency also has responsibilities for relations with the private sector and research issues

### ***Public and Private CERTS (Computer Emergency Response Teams)***

CERTS (Computer Emergency Response Teams) are specialized organizations, built to handle IT security incidents, in order to monitor, prevent, detect computer security incidents and circulate information about them. There are over 100 CERTS active in the EU, but their geographical distribution is very uneven. Almost all countries have 1 or 2 public sector CERTS, responsible for governmental or national research/education networks. But there are also a significant number of private CERTS in Germany and the UK, which are typically owned and organized by telecommunications operators, ISPs, banks, or industrial companies. These private CERTS primarily provide services to their owners, but may also participate in national or international forums. Some of them have different acronyms for example CSIRT (Computer Security Incident Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team), SERT (Security

Emergency Response Team), but the main scope remain the same. Over the years, CERTS extended their capacities from being a mere reaction force, to acting as a complete security service provider, including prevention services such as alerts, security advisories, training and security management services.

Some CERT are active at the national level, acting as an IT security point of contact (PoC) for a country. In most cases this role is fulfilled by the governmental CERT, which serves government and public sector agencies. An example might be US-CERT8 that acts as a PoC for the United States and is supported by the CERT/CC in delivering its services. Governmental or national CERTS are also dealing with CIIP issues, or collaborating with CIIP bodies.

In the United Kingdom, UNIRAS, the governmental CERT is a part of NISCC (National Infrastructure Security Coordination Centre), and as such is responsible for Critical National Infrastructure protection.

In Finland, CERT-FI is the national CERT for the whole of Finland, including government and critical national infrastructures, and acts as the alert, warning and response component of FICORA (Finnish Communication Regulatory Authority).

CERTS mostly share operational security incident data, but sharing of trend data is not their primary objective. They are also organized in a supernational organization, FIRST (International Forum of Incident Response and Security Teams), whose scope is to develop and promulgates best computer security practices, share the combined knowledge, skills and experience of its members (195 teams in 43 world countries) and to promote a safer and more secure global electronic environment.

Examples of collaboration between CERTs involve also private incident handling initiatives (or Private CERTs), which typically are owned and organized by ISP's, banks, multi-national or industrial companies. Those private CERTs provide services to their owners, as in the case of the BT Computer Emergency Response Team. The BT CERT coordinates analysis of software and hardware vulnerabilities, distributes bulletins, alerts and related security information, provides international and national information on vulnerabilities. BT CERT participates in the research of security tools and is a member of the Forum of Incident Response and Security Teams (FIRST).

### ***CIIP (Critical Information Infrastructure Protection) Bodies***

In all countries, critical infrastructures (transportation, finance, electric power, water, emergency/rescue services, health services) are increasingly dependent on the evolving information infrastructures (the public telephone network, the Internet, and terrestrial and satellite wireless networks) for a variety of information management, communication, and control functions. These information infrastructures (the critical infrastructure ICT systems and networks) are highly vulnerable to attacks, including cyber-crime attacks, so they need specific attention and protection measures.

The main actors dealing with issues related to the governance of CIP (Critical Infrastructure Protection) and CIIP (Critical Information Infrastructure Protection) come from different environments and have different responsibilities (as stated in the International CIIP Handbook).

1. Many of these actors belong to the public sector. Public CIP/ CIIP bodies help Governments in their complex tasks of controlling national overall security and protect public safety. In case of an emergency or crisis, they contribute to insure the effective functioning of the economy and the continuity of government services. These bodies are also involved in the assessment of potential risks and threats, and the definition of adequate responses by government.
2. The academic community does research into different fields of CIIP, ranging from technical issues to political or economic aspects. Until now, CIIP has mainly been a topic for engineers, IT security specialists, and other experts, while the sociopolitical dimensions of the topic have been rather neglected.
3. Some CERTs with national responsibilities play a supporting role assisting critical information infrastructure providers and government regulatory bodies in identifying and addressing information security vulnerabilities and threats.

However, critical information infrastructures are mainly run by private operators (also due to the ongoing privatization of service providers in vital sectors such as water, energy, or transportation). This means that the CIIP bodies cannot have the main responsibility over the infrastructures, which belongs to the operators owning and managing them. In practice, public bodies may monitor, advise and identify operational requirements, but the infrastructure operators maintain the final responsibility to implement effective protection policies.

Given this scenario, the protection of critical information infrastructures requires cooperation and information exchange within public-private partnerships, especially when dealing with threats and risks that exceed ordinary business risks. Also international co-operation should be required, when vital infrastructures cross physical or virtual borders.

This kind of cooperation is not easy to achieve. The CIP (Critical Infrastructure Protection Project) in the Netherlands performed a scan to map out the critical sectors, products and services in the country, identifying the key junctions between critical sectors and services, mapping out the vulnerability of sectors and junctions, developing a cohesive set of protective measures. This project concluded that organizing public-private co-operation on critical infrastructure protection requires a strong vision and leadership by the government. Cooperation is vital as there are in CIP many inter-dependencies of vital products and services. Cascading effects due to failure of one infrastructure may occur due to the dependency chains.

The expected adoption of a new EU Directive for Critical Infrastructures will help to identify these infrastructures and set up appropriate institutions for governance and guidelines definition in each Member State. But the Directive does not foresee strict obligations for individual organizations. It is likely that more time will be necessary (at least 5 years), before all European MS will achieve an agreement over common measures and actions to be taken to improve the security of critical infrastructures.

---

### **University and Research Institutions**

Higher education and research institutions perform a critical role for the NIS market, by carrying out applied and long-term research in the field and by educating the necessary human resources.

In many European universities, IT Security is a top priority research area. Security Labs are typically part of the Computer Science Department, but they can also be found in Engineering, Mathematics or other faculties. University research spans from theory to practice: from the theoretical foundations of cryptography (originally developed in University labs, as many other Security inventions) to the development and analysis of cryptographic protocols and algorithms, systems security, network security. Universities study IT security issues not only from a technological point of view, but as a multidisciplinary field, with legal, regulatory and societal implications. Many business and management universities feature NIS process or management courses.

Through their networking and knowledge-sharing activities, universities and research centers perform an essential role for innovation development, technology transfer to EU enterprises for the creation of new products and services (thereby contributing to their competitiveness), and training and awareness raising among business users, especially SMEs. The best security labs generate spin-offs or start-ups who may progress to become dynamic, new-technology based enterprises.

---

### **Standardization and Certification Bodies**

Standards development is particularly relevant for the ICT industry, given the trend towards interoperability and integration of networks. Security is clearly an important feature of any network, so standardization bodies typically have specific Work Groups dedicated to security standards development. The NIS activities carried out by the most important standardization bodies are the following ones:

- **The International Organization for Standardization (ISO):** The NIS work is carried out in the Joint Technical Committee of ISO and IEC (International Electrotechnical Commission): Subcommittee SC 27 IT Security techniques (in short, JTC 1/SC 27). An important piece of work that is currently under development concerns the family of Standards for Information Security Management System (ISMS), the so-called 27000 Family.

- **The European Telecommunication Standardisation Initiative (ETSI).** Within ETSI, the TISPAN Working Group (WG) 7 is in charge of the security of the Next Generation Network (NGN) architecture. The Smart Card Platform (SCP) Technical Committee takes care of the standardization of smart cards, with successful examples in the specifications of smart cards such as the SIM (Subscriber Identity Module) card in GSM and the USIM (Universal SIM, ETSI TS 131 102) card in UMTS. SCP focuses on developing an Integrated Circuit (IC) Card platform for mobile telecommunication systems, which can work for multiple applications. SCP has clearly great relevance for several business areas, e.g. e-commerce.
- **The ICT Standard Board (ICTSB)** is a collaborative group of organizations supporting ICT standardization by making proposals and recommendations. Within ICTSB, the Network and Information Steering Group (NISSG) gathers experts with the task of NIS standardization coordination.
- **The Internet Engineering Task Force (IETF).** The IETF is an international community working for the development of the Internet architecture and standards. Security has gained an important space within the design work of the Internet, and IETF has a dedicated Security Area comprising a number of Working Groups.

Technical staff dedicated by the most important ICT suppliers and technical government bodies participate to the working groups within these standardization bodies. They play a very important role, by negotiating agreements and dealing with conflicts among competitors allowing the development of open standards and interoperability of proprietary technologies. They provide essential guidelines and recommendations to governments and the main public bodies. A very important part of the competitive positioning game is decided in these offices and labs. ICT standards development, including NIS aspects, raises important policy challenges. For example, innovative ICT SMEs are under-represented in standardization bodies, and may find themselves at a disadvantage because of certain technical standard choices. European Commission Vice-President Günter Verheugen recently indicated that the Commission is considering the revision of current legislation to establish a strategic policy platform for ICT standardization, to take into account these and other issues (concerning for example IPR issues in the software industry). This will obviously include NIS standards development.

---

### **Lawyer Firms and Insurance Companies**

Lawyer Firms are clearly involved to consult and advise government organizations on the IT security regulatory framework, but they also play an important role providing specialized legal services to the main vendors and to medium-large business users on issues such as liabilities for IT security breaches. There is also an increasing demand

by business users for specialized insurance services addressed to IT security risk mitigation.

---

### **Professional and End User Associations**

There is a very high number of professional, industry and end user associations active in the security market and engaged in a dialogue with the EC and policy makers. They are:

- Professional associations (such as CLUSIF, Club de la Sécurité de l'information Française) aim at sharing information and experiences of risk management and improving skills;
- Industry associations (such as EICTA, the European ICT industry Association) represent the interests of their associates and dialogue with policy makers to influence the regulatory framework;
- Consumer groups and Internet users associations aim at rising awareness to fight cyber crime and/or to help citizens to protect privacy and personal data. A domain where NGOs are particularly active is children protection over the Internet and finding ways to prevent and fight paedophiles on the Net.

Finally, the Internet world includes several professional and opinion groups with contrasting positions about IPR policy, particularly the role of software patents, software piracy, and/or copyright violations of digital content (illegally downloading music or films for example). These debates influence the competitive scenery and the development of the Internet regulatory framework, and affect indirectly the NIS scenario.

- Some of these stakeholders campaign to defend the Internet environment from excessive regulation, restraining information and knowledge circulation, such as the FLOSS (Free/Libre/Open Source Software) movement or the Foundation for a Free Information Infrastructure, (FFII). The OSS (Open Source Software) movement supporters believe that the free circulation and licensing approach weakens the reasons to carry out software piracy, that software diffusion is good in itself, even if they do not agree with copyrights violations in principle.
- The stakeholders in favour of software patents and strong IPR protection (for example the BSA, Business Software Alliance) believe that software piracy creates economic damages, limits the growth of the industry and must be fought with all possible means. These stakeholders push for more effective regulation and its implementation.

### 3. MAIN DRIVERS AND BARRIERS OF THE NIS MARKET: STAKEHOLDERS OPINIONS

#### Profile of Stakeholders Interviews

The study team interviewed 12 opinion leaders from the main stakeholder categories (excluding suppliers and users, already covered in the surveys) to provide input on critical issues and depth to the qualitative analysis. The main criteria for selection were:

- Interviewee with recognized expertise, status and role in their category
- Vision of problems at the EU/international level, rather than simply domestic

The list of interviews is reported below. Some of the respondents preferred to remain anonymous.

**TABLE 2**

List of Stakeholders Interviews

Stakeholder Categories	Interviewee	Role
University and Research	Babak Akhgar	Professor of Information security and Informatics, Sheffield Hallam University, United Kingdom
Standardization and Certification Body	Charles Brookson	Chairman GSM Association Security Group, United Kingdom
Regional Government	Dave Fortune	Yorkshire Police Chief inspector and Police Seconded at Yorkshire Forward (Yorkshire Development Agency)
Professional and end-user associations	WM Hafkamp	Rabobank group, responsible of banking association for security, Netherlands
Philanthropic, Educational and Professional Associations	Pascal Lointier	President of CLUSIF (Club de la Sécurité de l'Information Française), France
Business Services / Insurance	Lorenzo Missaglia	Allianz S.p.a, Head of Fire, Electrical and IT insurance policies MID-Corporate,
Legal assistance	Peter Van de Velde	Bird & Bird, Senior European Counsel, Member of the Brussels Bar
Public and private CERT	N.A.	Chief Security Officer of a New Member State national CERT
Public and private CERT	N.A.	Chairman of the Board of a New Member State national CERT
Business Services/Insurance	N.A.	Manager, Leading European Insurance Company
CIIP (Critical Information Infrastructure Protection) Bodies	N.A.	Officer, Institute for the Protection and Security of the Citizen (IPSC) of the Joint Research Centre (JRC), European Commission
Public Network and Information Security Body	N.A.	Security Expert of a leading European National Security Agency

N.A. = Not Available. These Interviewees asked to remain anonymous.

Source: Summary of Stakeholders Interviews, Government Insights, 2008

## **Opinions on Main Drivers of Demand**

The stakeholders have quite strong opinions on the main drivers and barriers of the development of the NIS market (*main opinions are summarized in the following table*).

There is a general consensus that the main driver is the growth of Internet use, because the Net is inherently insecure, with new threats and risks emerging in parallel with new innovation and services. The trend towards greater openness and integration of networks and information infrastructures, with increasing interoperability, inevitably opens the way to new weaknesses and vulnerability, creating the need for more advanced security measures. Fear or direct experience of attacks is also an important factor driving users choices about NIS products and services.

At least two stakeholders underlined the increasing relevance of security for mobile communication networks, where authentication and identification problems are even more delicate than for fixed networks. Mobile phones today are low-cost consumer products, which makes it more difficult to add even a small additional cost to improve their security.

Compliance with legal requirements, as a driver to adopt security measures, was mentioned by many, particularly by users' associations representatives, referring mainly to data protection and privacy protection laws and directives. Interestingly, one stakeholder indicated the development of eGovernment as a driver of demand, because of the new requirements for NIS posed by online public services. The JRC representative pointed out that public procurement of security solutions is expected to increase, therefore driving market growth.

One of the CERT manager, underlined that EU level cooperation is particularly important for the New Member States, who are setting up their infrastructures and services to protect themselves against NIS risks and profit from know-how and consulting support from other, more experienced European actors.

Overall, the opinions of the stakeholders about the drivers of the NIS market are remarkably similar, based on an apparently shared vision of the market trends.

There are many common elements in the stakeholders views about the barriers of the NIS market as well, but based on different evaluations about the relevance of the different elements. The two most important barriers are identified by all as the perceived high cost of security products and services, and the lack of knowledge (not of awareness) about threats and protection measures. Stakeholders closer to the user side indicate costs as the most important problem, while regulators and public bodies are more concerned with the lack of awareness and knowledge.

According to the stakeholders, there is a generic awareness about potential IT security risks, but very vague and apparently not able to lead to appropriate behaviors. This means that users are not well able to measure the benefits of security products and services, and therefore its cost is always perceived as too high. These two elements are closely related, but in a very different way depending on the type of user, that is for consumers, SMEs or medium-large organizations. In practice, the stakeholders point out that:

- Consumers appear to be little aware of threats, and easily convinced that the purchase of simple products is sufficient to protect them. The president of CLUSIF, the association of French security users, mentioned for example a recent survey where users proved to be at the same time amazingly ignorant, but convinced to be protected.
- SMEs are more aware of the existence of potential threats, but almost as much in the dark as consumers about the actual level and type of risks. They lack skills and competencies in this field, but must also comply with regulation.
- Medium-large enterprises are considered to be more aware, but rarely carry out a proper cost-benefits analysis of NIS risks and in any case lack the instruments to measure them. As one stakeholder said, well-founded business cases for the ROI on security investments are very much lacking. Top business levels are not well prepared about NIS risks relevance.

But are security costs really too high? According to the stakeholders it is not simply a problem of perception. As always in the case of risk management, total protection is extremely expensive, so there must be an evaluation of reasonable protection vs reasonable costs, based on objective data about potential damages. This knowledge is unfortunately missing, since comparative risks assessment, including an evaluation of potential damages, is difficult and usually not applied to SMEs and consumer markets. But there is also some criticism of offering pricing policies, which do not seem well suited to the main user categories needs (*see also the following considerations about main challenges*).

The role of regulation is also criticized. Regulatory obligations to prevent NIS threats are still uneven across Europe (excluding the data protection directives). Some regulatory measures impose formal compliance without actually insuring protection; the focus should be more on requiring a minimum level of security rather than adopting standards or measures. From the point of view of the mobile markets, some important initiatives (for example the IMEI database for mutual authentication of mobile users at the international level) have been recognized and adopted only by few Member States. As the CIIP expert mentioned, European level guidelines (such as those existing for example in the US) would be useful.

**TABLE 3**

## Stakeholders Opinions on NIS Market Main Drivers and Barriers

Interviewee	Main Drivers	Main Barriers
Babak Akhgar	User driven demand both at organizational and national level; Technology availability and product awareness; National and international security lapses such as terrorist attack on ICT infrastructures (e.g. cyber attack on critical networks)	Legal requirements such as data protection and privacy issues; Technological failures; Lack of trust in providers and consumers of NIS services and products, at all levels of the NIS supply chain (including national repositories).
Charles Brookson	Prevention of fraud to consumers and operators; Ensuring the security integrity of networks; Compliance with regulations; Business needs related with security (i.e. mobile operators need to protect identity data)	Relatively high cost required to provide really good security levels, and the unwillingness of consumers and organizations to pay for that extra security; Limited diffusion of legislation about security measures implementation in the mobile market (IMEI database management)
Dave Fortune	Global trading on line; Fast changing of technology; Increase of diversity of threats	Not updating security; Lack of transfer of knowledge/cooperation between industries and security agencies; Constant evolution of requirements
Security Expert of a leading European National Security Agency	Growth of the Internet and ubiquitous computing with increasing threats for data	Diffusion of proprietary, not interoperable solutions in the ICT field which may hinder the entry of new competitors and market growth.
WM Hafkamp	Growth of the Internet and of Mobile services, via virtual channels; privacy requirements driving demand for authentication	Regulations may become barriers, for example the SEPA standard effects are not clear
Pascal Lointier	Legal requirements (e.g. data privacy regulation), Security breaches reported by the Media; Growing integration and interoperability of ICT networks creating the need to regulate and control data flows; Impact of new technologies (new services and new threats)	Some legal requirements are putting too much emphasis on specific aspects, and are not helping organizations to have the right approach towards Security; organizations are not properly organized to address Security issues. Most of them have never done a proper analysis
Peter Van de Velde	Compliance is a driver of investment in Security measures, but not only in technical measures. Organizations need a great help to understand what are the norms they need to apply, so there is a need also of consultancy to be compliant.	
Representative of a New MS national CERT	Big security incidents	Fighting global problems locally is a barrier for the development of this market
Representative of a New MS national CERT	e-Government, online public services impose new security requirements both to public agencies and to users; the growth of the Internet which is inherently insecure	Insufficient knowledge by end users of security threats and protection measures. Monoculture in software products. Lack of European guidelines: Insecurity of the current mechanism for domain names registration

**TABLE 3**

## Stakeholders Opinions on NIS Market Main Drivers and Barriers

Interviewee	Main Drivers	Main Barriers
Officer of a CIIP body	Higher usability of Security products and services; Public procurement driving higher investments; Fear or experience of serious attacks, with relevant business/national security consequences.	High ignorance of the real dimension of Security problems by SMEs and consumers, while large firms lack precise information over risks, threats, attacks data; Lack of preparation/training in security matters, particularly evident at top business level; high costs of Security (in terms of human resources, equipment, services).

Source: Summary of Stakeholders Interviews, Government Insights, 2008

### Opinions on the Main Challenges for the Market Development

The stakeholders were asked to indicate the main challenges for the development of the NIS market in Europe. These challenges correspond to the main problems identified by the interviewees.

The first and most important challenge appears to be the development of "a better business case for security investments" as the JRC expert describes it. To do this, many stakeholders point out that there is a need for appropriate methodologies and tools to assess security risks and the cost-effectiveness of security investments in the business environment, as well as better practical knowledge of security threats in the home. But it is also important that enterprises see the need for and implement better security management techniques. Part of the responsibility, though, is attributed to suppliers, because of the difficulty "to find a security solution with the right cost-benefits balance". In other words, even if the users learn to use the right risk-assessment methods, the offering responding to their needs may be missing. At least two stakeholders mention, among the challenges, the need to improve the reliability and user-friendliness of NIS offering, and the pricing policy. The fast development of the market, its high rate of technological innovation and its global dimension create a problem of standards and regulation development at the same speed, to cope with new and emerging trends. Other challenges are related with the difficulty to implement the appropriate incentives for an effective NIS management. For example, the CIIP expert points to the need of clarifying the responsibilities of organizations that do not invest sufficiently in security and therefore cause or receive damage (this would increase the incentive for security investments).

The President of CLUSIF mentioned also that regulatory compliance in this field is sometimes more geared toward formal respect of rules, rather than genuine attention to protection against risks. Other challenges are the development of stable standards and of more comprehensive guidelines for users. The CERT representative underlines the need for more research and development, and for

greater coordination of NIS implementation in the field of e-government and online banking. While Mr Van de Velde highlights the new challenges due to the shift from computer-assisted crimes to frauds committed with the help of ICT technologies, towards criminal behaviors that are directed against computers and networks.

**TABLE 4**

Stakeholders Opinions on NIS Markets Development Main Challenges

Interviewee	Main Challenges
Babak Akhgar	Justification of ROI in security initiatives, technology maturity and Trust Management (i.e. trust in consumers and providers of NIS as well as protective measures such as legal and legislative issues)
Charles Brookson	Improve the information and awareness of users about protection measures; Difficulty to secure old legacy ICT systems; significant challenge of finding a security solution with a right cost-benefits balance
Dave Fortune	Technological reliability/robustness and ease of use; Pricing policy (creation of a competitive environment); Reduce the domination of few players
WM Hafkamp	Lack of user friendliness of security products and services; for banks, need to find the balance between risks and security investments
Pascal Lointier	Organizations perceive Security as a cost, not an investment, missing tools able to measure the real impact of incidents and security interventions; lack of awareness; defining a minimum level of security, instead of imposing generic compliance of standards providing insufficient protection; Improving the practice of security
Peter Van de Velde	There is a shift from computer-assisted crimes (as spamming, piracy and identity theft), frauds committed with the help of ICT technologies, towards criminal behaviors that are directed against computers and networks, as in the case of Denial of Services. ICT systems are not the tools but the target of disruption.
Security Expert of a leading European National Security Agency	Need greater support for innovative enterprises in the field (start ups); growing but insufficient use of security products by consumers; constant need of new standards because of technological innovation, to support market development
Representative of a New MS national CERT	Turn local actions to global cooperation, standardization and interoperability are not a problem for the development of the market, and he doesn't think technical innovation will launch a new phase of growth in the market
Representative of a New MS national CERT	Need for more research and collaboration, and a strong demand of coordinated activities in the field of eGovernment systems and Online banking. In Eastern Europe lack of CERTs and Central bodies(due to insufficient resources and knowledge). Lack of awareness by consumers
Officer of a CIIP body	Need to clarify the responsibilities of institutions who did not take sufficient protection measures; Definition of stable standards, de jure or de facto, to help firms select solutions and improve interoperability (also guidelines like in the US); need to develop a solid business case for Security investments.

Source: Government Insights, 2008

---

## **Opinions on NIS Market Supply-Demand Match and Maturity**

The stakeholders' opinions about the match demand-supply are remarkably similar. They all consider that the present offering is fairly satisfying for large enterprises, moderately satisfying for consumers (who are not very demanding, though) and definitely unsatisfying for SMEs. But the President of CLUSIF points out that also large enterprises find the NIS offering rather rigid, with many CIO complaining that their organizations must adapt to the offering, instead of the opposite way around. Concerning SMEs, the stakeholders agree that the existing offering does not seem well-suited to their needs, that they lack the specific knowledge to select the right product/solution for their needs, and do not receive much support from NIS vendors on this. The NIS market is still in development and is not considered mature yet. Growth is expected, both from the enlargement of the market (more users) and its deepening (purchase of more products by existing users, with more intensive use). Professor Akhgar of Sheffield University estimates that the EU market maturity is behind that of the US one. The stakeholders agree that the European market is varied and with many different national regulation and conditions. However, they were not willing to point out specific rankings or classifications of maturity. It seems that the fragmentation of the market affects also the experts' view, as they have difficulty to have a complete vision of the variations across the EU. One of the stakeholders pointed out that a single market for security would enable the emergence of stronger European players.

**TABLE 5**

## Stakeholder Opinions on NIS Markets Maturity and Match Demand-Supply

Interviewee	Match Demand-Supply	Maturity
Babak Akhgar	Large business users level of satisfaction is fairly high, with variations across the EU. Their main problem is the lack of risk assessment at the national level. SMEs needs are not satisfied; they lack knowledge of security offering.	A growing market, both in terms of the number of users and the wider range of purchases by existing buyers/users. The EU market isn't as mature as the global market; it is behind the US one.
Charles Brookson	There are very different situations around Europe, for example the lack of legislation on IMEI (International Mobile Equipment Identifier) Database and uneven use by operators	The market is still in a growth and development phase in terms of innovation within the wireless sector, and this will require further security innovation to protect consumers and networks
Dave Fortune	Large business users are satisfied with present offering. Consumers are satisfied as long as e-business is guaranteed. SMEs are less satisfied; due to lack of funding for investments in reliable and user-friendly information security solutions.	The NIS market is evolving but is far from saturation and maturity. Fast technological evolution, change of threats, change of demand requirements due to increase of demand maturity level can help the future growth.
Pascal Lointier	Many CIO complain that they cannot find security solutions that fit with their needs: they have to adapt the organization internal processes and activities to respond to the way security products work. SMEs often lack specific advice and support from the vendors on the best selection criteria of a security product or solution for their needs.	
Security Expert of a leading European National Security Agency	ICT security is a difficult and complex field. Not being user-friendly is partly system inherent. An adequate awareness for ICT security would increase acceptance for user-inconvenience. Our agency works together with manufacturers and offer certifications to improve trustworthiness, raise awareness and increase market transparency to finally reduce any false sense of protection and convert it to an adequate sense of protection.	The market is not actually mature, is still in development. There is a constant trend towards consolidation, resulting in many small companies being acquired by large vendors.
Representative of a New MS national CERT	Users are asking for more user-friendly security products. Also they need to be educated and helped to use those products. Offering is often inadequate (particularly one-in-a-box solutions)	
Representative of a New MS national CERT	Large business, SMEs and Consumers users are satisfied with NIS offering, also because their expectations are low	Most users and supplier believe that the market is already mature but attackers see it opposite. Large businesses are much more aware and evolved in terms of adoption of security than SMEs.
Officer of a CIIP body		A single market for security is the only way to allow the development of some significant European industry players. In order to achieve it, it would be advisable to set similar rules and regulations across borders.

Source: IDC synthesis of stakeholder Interviews.

## 4 OPINIONS ON THE REGULATORY FRAMEWORK OF THE NIS MARKET

The opinions of the stakeholders about the regulatory framework at the national and European level present some important variations.

The prevalent opinion seems to be that there is a lack of coherence between the national and EU level of regulation. However, only the JRC expert underlines the need for more and better regulation at the EU level, to fill the existing gaps, especially for the protection of Critical Information Infrastructures. Public bodies representatives deny the need for more regulation. Most stakeholders favor an approach based on better implementation, rather than more regulation. The BSI representative suggests a bottom-up approach based on agreement among Member States. The president of CLUSIF and professor Akhgar agree that there is a major problem in the lack of enforcement of existing regulation and weak prosecution of security violations, with low penalties. The EC is criticized because of the lack of advice and support to organizations with security problems. Mr Brookson, representative of the GSM association, reminds that when implementing global standards and technologies (as is most often the case for ICT products and services) the variety of national regulation becomes a serious obstacle. Therefore standard organizations try to focus on minimum indispensable requirements. This observation implies an appeal for streamlining and simplifying regulation in this field in Europe. The stakeholders were asked an opinion about an Observatory of the ICT market, based on a public-private alliance, able to release every year data and evidence about the development of the NIS market. Most of them were interested, but with a certain scepticism about its feasibility and likeliness. There were no proactive suggestions about the best way to initiate it and which stakeholders could be willing to provide funding for it. The manager of one CERT pointed out that providing knowledge and data about the market would make more sense if a single regulatory space were achieved in this field. More resolved is the other one manager. He affirms that it's not interested to the creation of an Observatory of the ICT security market.

**TABLE 6**

Stakeholder Opinions on Cooperation at the EU level

Interviewee	Opinions on the EU Regulatory Framework	Public-Private cooperation for an Observatory of the NIS market
Babak Akhgar	The current regulatory framework in the UK is progressively addressing security, as problems are arising, but not in a satisfactory manner. The main problem is a lack of enforcement, so that illegal actions are not well prosecuted. He agrees with Mr. Lointier's opinions.	No answers but availability to participate at the observatory.
Charles Brookson	The GSMA position is to try to comply with all minimum requirements as a baseline. Some of the areas of concern include customer privacy, handset theft, and lawful interception.	The Observatory of the ICT security market seems a good idea and I would support it. There may be problems of feasibility.

**TABLE 6**

## Stakeholder Opinions on Cooperation at the EU level

Interviewee	Opinions on the EU Regulatory Framework	Public-Private cooperation for an Observatory of the NIS market
Dave Fortune	Level of coherence between the EU, national and regional/local level of the NIS regulatory framework is low.	Better information and knowledge about the trends in the ICT security market at the EU level is and should be promoted. The Observatory of the ICT security market could be a good opportunity for fostering new technological solutions as well as rules and best practices.
Pascal Lointier	The current regulatory framework is sufficient. The main problem is lack of enforcement, so typically illegal actions are not well prosecuted, and applied penalties are often too low, without a discouraging effect. Furthermore, EU authorities have proved to be slow in providing publicly available advice or to help organizations responding to Security issues.	Networking activities among state agencies and associations should be more frequent.
Peter Van de Velde	The Data Privacy Law, that sets specific rules over the protection of data, had an high impact and is actually one of the most efficient laws to prevent security braches and loss of customers data. Enforcement is still not sufficient. Enterprises are protecting themselves also via legal actions, against malicious activities done both by external and internal (employees) hackers, but they tend not to declare they have been subject to some loss of data or interruption of services, that could be attributed to scarce security of systems and procedures.	
Security Expert of a leading European National Security Agency	Security in the EU is a matter for single Member States. It would be counterproductive to produce more European regulations in this field with a top down approach. It would be much better to establish a bottom up approach, enabling single Member States to agree - in a multi-lateral way – to common standards and solutions to ICT Security issues.	In our experience collaboration is not a problem. Concerning an Observatory of the market, more information and transparency is crucial so it would be a good contribution to ICT security but is not an easy task.
Representative of a New MS national CERT	As regards the need for more or less regulation at the EU level, this is not a question about EU, problems are global, so the solution has to be also global	Not interested to the set up of an Observatory of the ICT security market at European level.
Representative of a New MS national CERT		It is not worth speaking of a single market but more of a single regulatory space. In that case, if effectively achieved, it could be useful both for users and vendors.
Officer of a CIIP body	More regulation is needed, to establish security baselines and requirements for systems in private hands that can affect society at large. There is a need for greater coherence at the level of European systems/infrastructures. More regulation is expected, and needed, for Critical Infrastructure Protection.	There is a need for better information and knowledge about the trends in the ICT security market, mainly in the context of the whole security market. But it should be a private initiative with the support of governments. R&D should play a secondary role. It should be linked to standardization (formal, semi-formal) initiatives.

Source: IDC synthesis of stakeholder Interviews.

## **The emerging IT security Insurance Services Market**

There is an emerging market of business insurance services aimed at transferring IT risks (direct and indirect losses, as well as civil liability deriving from the supply of software or IT services), as a way to reduce the possible negative consequences in case of failure of the systems or unexpected events. Insurance is not alternative to the implementation of IT security solutions, rather is one more tool for an efficient IT security management. In other words, firms should use insurance policies to cover “residual risk” (risk not covered by ad hoc technological and organizational countermeasures).

The main companies offering these services in Europe are Allianz, Generali, AIG, ACE Europe, Zurich and few others (with lower market shares). The market value is still small, estimated by industry actors at around €10M in countries such as France, Germany or Italy. It is basically a specialized niche market and likely to remain so.

Enterprises likely to use this kind of insurance are:

- IT service providers (network connectivity, housing & hosting, remote data processing, etc) and software houses;
- Large IT departments of banks, insurance companies, hospitals, government organizations.

In the first case, IT risks insurance is important for the core business, and is practiced also by small firms. All IT and TLC service providers need to protect themselves from possible huge losses, due especially to civil liability versus third parties (i.e. customers, citizens), for example for loss of service. Of course insurance cannot prevent the company from other indirect damages (loss of image, loss of the customer, internal costs incurred to find a solution to the problem).

In the case of firms out of the ICT industry, there is a growing trend among large service providers to underwrite IT insurance policies, which are often embedded in larger policies. SMEs in the same sectors are much less likely to do so, probably because they consider the insurance costs too high. These firms prefer to rely on IT security products and services only.

IT risks insurance is not heavily regulated, save for some specific areas (for example, certification authorities issuing digital certificates must be covered by an insurance policy).

**TABLE 7**

## Stakeholder Opinions on Insurance Services for the NIS market

Interviewee	Benefits from insurance	Main User sectors	Can Insurance services substitute for NIS products and services?	Level of regulation
Manager, Leading European Insurance Company	Through an insurance policy companies can transfer the majority of risk deriving from the use of IT. This of course does not eliminate all the inconvenience and negative impacts of a security accident	IT service providers (network connectivity, housing & hosting, remote data processing, etc), Software houses, Large IT departments of banks, insurance companies, hospitals, public administration.	No. Information security applications/systems and IT Security policies must be seen as complementary, not as alternative solutions.	Some particular areas are subject to specific regulation (for example, certification authorities issuing digital certificates must be covered by an insurance policy).
Lorenzo Missaglia	Reduction of costs deriving from loss of data, reduction of costs deriving from denial of service..	The NIS market is still a niche market for insurance companies, and is going to remain a niche market for a long time. Sensitivity versus information security insurance services is quite low, except for very large companies in some industries (banks, telc os, large IT services outsourcers).	No. From a conceptual point of view, firms should use insurance policies to cover "residual risk".	The level of regulation is quite low (with respect to other insurance sectors)
Peter Van de Velde			There is a growing demand of insurance services to address issues coming from the insecurity of ICT systems, computer and networks. There are already insurance offerings, not for cybercrime but any way addressed to cover ICT risks	

Source: IDC synthesis of stakeholder Interviews.

### **The case of Estonia and the emerging threats of cyber-attacks**

Between April and May 2007, Estonia, a small Baltic country but also one of the most wired countries in Europe (with many "e-society" and online services, such as paperless government and e-voting), was subject to massive, well coordinated, targeted series of cyber attacks on Web sites of public (government) and private organizations (banks, telecommunications companies, Internet service providers, newspapers). This episode was the first case of Internet attack on a

country public and private information infrastructures and it created a great echo in the media and in the security market. This case underlined the potential vulnerability of information systems and raised worry about the use of cyber attacks as new weapons in international conflicts.

In the case of Estonia, the cyber-attack lasted 3 weeks and came close to shutting down the country's digital infrastructure, clogging the Web sites of the president, the prime minister, the Parliament and other government agencies, the biggest Estonian bank and several daily newspapers. Most of the attacks that had any influence on general public were distributed denial of service type attacks ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred. Hackers were using botnets (bots are computers that can be remotely commanded to participate in an cooperative action). Roughly 1 million unwitting computers worldwide were employed. Officials said they traced bots to countries as dissimilar as the United States, China, Vietnam, Egypt, and Peru.

Mr Hillar Aareleid, Chief Security Officer of the Estonia's Computer Emergency Response Team (CERT-EE), decided to erect firewalls around government Web sites and set up extra computer servers. He also gathered security experts from Estonia's Internet service providers, banks, government agencies and the police. Internationally, he drew on contacts in Finland, Germany, Slovenia and other countries, to help him track down and block suspicious Internet addresses and halt traffic from computers as far away as Peru and China. This coordinated response was effective and served to halt the effects of the attack.

The origin of the attacks was never clearly identified. But it all started after the Estonian authorities began removing a bronze statue of a World War II-era Soviet soldier from a park in Tallin, the Estonian capital. This move was seen as an offense to the memory of Russian soldiers killed in WWII by the Russian government and population, as well as by the large minority of ethnic Russians living in Estonia (a quarter of the population). This increased again the level of tension between the two countries, due to past history and also to the Estonian policy towards the Estonians of Russian origin.

For these reasons, the Estonian government accused Russian hackers of the attack and the Russian government to have organized it. But the involvement of Russia in the attacks is not proven, as professional hackers could easily have used Russian IP addresses to spoil relations between Estonia and Russia. However, it seems likely that Russian hackers were behind most of the attacks. At least one was found guilty by a tribunal and condemned to pay a fine: Dmitri Galushkevich, an ethnic Russian student living in Tallinn, who in January 2008 was found guilty of participating in the assault, attacking the website of the Estonian Reform Party.

The Russian government officially denied any involvement in the attacks. Expert opinions tend to confirm this. For example, professor James Hendler, former chief scientist at The Pentagon's Defense Advanced Research Projects Agency characterized the attacks as "more like a cyber riot than a military attack." Experts interviewed by IT security resource SearchSecurity.com "say it's very unlikely this was a case of one government launching a coordinated cyberattack against another". On the other hand a few hackers anonymously quoted in the media admitted that there may have been "recommendations and suggestions" from Russian authorities to the hackers, playing on spontaneous indignation and feelings of nationalism.

The emerging threat of cyber attacks has led to a response by the NATO, particularly because of the attacks on Estonia, a member of the organization. After the 2007 attacks, allied defense ministers pressed for a NATO cyber defense policy at their October 2007 meeting. This led to the creation of a Cyber Defense Center, which was announced by a NATO official statement on May 15, 2008. The Cooperative Cyber Defence Center of Excellence will operate out of Tallinn, Estonia with a staff of 30, to carry out research and help fight cyber warfare. Half of the specialists at the center will come from its seven sponsoring countries: Germany, Italy, Spain, Latvia, Lithuania, Slovakia and Estonia. The center will help NATO "defy and successfully counter the threats in this area" was said in the official statement. The Center is expected to be online since August 2008 and officially launched in 2009.

Previously, something similar (but less coordinated) happened with the Titan Rain series of attacks on the US information services after 2003, which were attributed to Chinese hackers, but were not coordinated and concentrated in a short period of time as the Estonian attack.

Military and IT security experts have discussed for years about the potential of cyber warfare, but the Estonian and Georgian cases have suddenly made it a real, rather than a hypothetical threat. There is disagreement on how to deal with cyber attacks, as real war or terrorism acts, or rather as a new kind of hooliganism, since they may come from non-state actors or independent hackers.

A professor of law at Temple University in Pennsylvania, USA, Duncan Hollis, thinks that there is a vacuum in international law about cyber attacks, since it is not clear how a state could or should defend itself, and whether for example NATO (a defensive alliance) was supposed to step in to help defend Estonia. Professor Hollis suggests that there should be a new "international law for information operations" to define a clear set of rules of defense: he also thinks that international organizations such as NATO should give the good example by agreeing to respect a clear set of rules.

Other experts believe that, given the unpredictable and spontaneous nature of these attacks, it is important to be prepared to protect vulnerable systems and information infrastructures and to counteract swiftly. A provocative, but stimulating point of view held by a few

digital security experts, is that greater use of open-source software may be the best way to build an effective defense, by enrolling the open source community to find and fix weak points of key software in websites or encryption algorithms.

In any case the threat of cyber attacks is now an important part of the security policy debate and must be taken into account by the EC.

---

## **Main Conclusions on Stakeholders Opinions**

The stakeholders interviewed represent public bodies governing the NIS market, users associations, standard associations, and university and research. Therefore they represent well the most important actor typologies, even if their opinions are still individual opinions. Notwithstanding their different roles, they present a strong convergence of opinions about the main drivers of NIS market development, which are the following ones, in decreasing order of importance:

- Internet market growth and its inherent lack of security;
- Regulatory compliance;
- Fear or experience of attacks.

There is consensus also about the main barriers, which are:

- High perceived cost of security products and services, related with the lack of tools for risk assessment and measuring potential benefits vs. damages;
- Lack of knowledge (not of awareness) about threats and protection measures, especially by consumers and SMEs.

The stakeholders agree also that the match supply-demand is different for the main user segments: large-medium enterprises are fairly satisfied, while the NIS offering for SMEs is inadequate. The offering for consumers may be even misleading, as there is no sufficient understanding by the users of the effective level of protection guaranteed.

The main challenge therefore appears to be the development of "a better business case for security investments" for the different users segments. Better understanding by the users and pricing/offering strategies closer to users needs are both needed. Regulatory compliance is also criticized for being too oriented to formal requirements, rather than substantial improvement of security levels.

The stakeholders differ mainly on their assessment of the regulatory framework and the role of the EU. Users' representatives point at the lack of enforcement of existing regulation and the need to improve implementation, asking for better support also at the EU level. They seem also interested in better operational guidelines at the international

level and cooperation between national/EU bodies. The university and research centre (JRC) stakeholders share this view and believe that CIIP particularly requires more EU-level regulation. Public bodies representatives deny the need for more EU-level regulation, because security policies are mainly of national interest, and suggest better cooperation at horizontal level among the Member States. Most stakeholders favor an approach based on better implementation, rather than more regulation.

The stakeholders consider an Observatory of the ICT market, based on a public-private alliance, with interest, but with some scepticism about its feasibility.