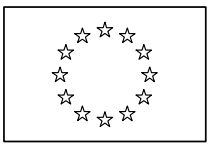

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 31.5.2006
COM(2006) 251 final

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"

{SEC(2006) 656}

CONTENTS

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"

1. INTRODUCTION

The Communication "i2010 – A European Information Society for growth and employment"[1], highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society.

The purpose of the present Communication is to revitalise the European Commission strategy set out in 2001 in the Communication "Network and Information Security: proposal for a European Policy approach"[2]. It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS).

Drawing on the experience acquired by Member States and at European Community level, the ambition is to further develop a dynamic, global strategy in Europe, based on a culture of security and founded **on dialogue, partnership and empowerment**.

In tackling security challenges for the Information Society, the European Community has developed a three-pronged approach embracing: specific network and information security measures, the regulatory framework for electronic communications (which includes privacy and data protection issues), and the fight against cybercrime. Although these three aspects can, to a certain extent, be developed separately, the numerous interdependencies call for a coordinated strategy. This Communication sets out the strategy and provides the framework to carry forward and refine a coherent approach to NIS.

The 2001 Communication defines NIS 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*". Over recent years, the European Community has implemented a number of actions to improve NIS.

The regulatory framework for electronic communications, the review of which is underway, includes security-related provisions. In particular, the Directive on Privacy and Electronic Communications[3] contains an obligation for providers of publicly available electronic

---

1 COM(2005) 229, 1.6.2005.
2 COM(2001) 298, 6.6.2001.
3 Directive 2002/58/EC.

communications services to safeguard the security of their services. Provisions against spam[4] and spyware[5] are laid down.

Trust and security also play an important part in the European Community programmes devoted to research and development. The 6th Research Framework Programme addresses these issues through a wide range of projects. Security-related research is to be reinforced in the 7th Framework Programme with the establishment of a European Security Research Programme (ESRP)[6]. Furthermore, the Safer Internet Plus programme supports networking projects and the exchange of best practices to combat harmful content circulating on information networks.

As a part of its response to security threats, the European Community decided in 2004 to create the European Network and Information Security Agency (ENISA). ENISA contributes to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union (EU).

The EU also plays an active role in the international fora addressing these topics, such as the OECD, the Council of Europe or the UN. At the World Summit on the Information Society in Tunis, the EU strongly supported the discussions on the availability, reliability and security of networks and information. The Tunis Agenda[7], which together with the Tunis Commitment sets out further steps for the policy debate on the global Information Society as endorsed by the world's leaders, highlights the need to continue the fight against cybercrime and spam while ensuring the protection of privacy and freedom of expression. It identifies the need for a common understanding of the issues of Internet security and for further cooperation to facilitate the collection and dissemination of security-related information and the exchange of good practice among all stakeholders on measures to combat security threats.

2. IMPROVING THE SECURITY OF THE INFORMATION SOCIETY: THE KEY CHALLENGES

Despite the efforts at international, European and national level, security continues to pose challenging problems.

Firstly, attacks on information systems are increasingly motivated by profit rather than by the desire to create disruption for its own sake. Data are illegally mined, increasingly without the user's knowledge, while the number of variants (and the rate of evolution) of malware[8] is increasing rapidly. Spam is a good example of this evolution: it is becoming a vehicle for viruses and fraudulent and criminal activities, such as spyware, phishing[9] and other forms of malware. Its widespread distribution increasingly relies on botnets[10], i.e. compromised servers and PCs used as relays without the knowledge of their owners.

---

4 Or unsolicited commercial communications.

5 Spyware is tracking software deployed without adequate notice, consent, or control for the user.

6 The ESPR is being prepared in the course of a Preparatory Action for Security Research during the period 2004-2006.

7 *Towards a global partnership in the Information Society: follow-up to the Tunis Phase of the World Summit on the Information Society (WSIS)* - COM(2006) 181, 27.4.2006.

8 Malware stands for "malicious software".

9 Phishing is a form of Internet fraud aiming to steal valuable information such as credit cards, bank account numbers, user IDs and passwords.

10 Botnets are networks of bots, which are applications that perform actions on behalf of a remote controller and are installed covertly on a victim machine.

The increasing deployment of mobile devices (including 3G mobile phones, portable videogames, etc.) and mobile-based network services will pose new challenges, as IP-based services develop rapidly. These could eventually prove to be a more common route for attacks than personal computers since the latter already deploy a significant level of security. Indeed, all new forms of communication platforms and information systems inevitably provide new windows of opportunity for malicious attacks.

Another significant development is the advent of "ambient intelligence", in which intelligent devices supported by computing and networking technology will become ubiquitous (e.g. through RFID[11], IPv6 and sensor networks). A totally interconnected and networked everyday life promises significant opportunities. However, it will also create additional security and privacy-related risks. While common platforms and applications contribute positively to interoperability and the take-up of Information and Communication Technologies (ICTs), they can also increase risks. For example, the greater the use of "off-the-shelf" software, the greater the impact when vulnerabilities are exploited or failures occur. The emergence of certain "monocultures" in software platforms and applications can greatly facilitate the growth and spread of security threats such as malware and viruses. **Diversity, openness and interoperability are integral components of security and should be promoted**.

The relevance of the ICT sector for the European economy and for European society as a whole is incontestable. ICT is a critical component of innovation and is responsible for nearly 40% of productivity growth. In addition, this highly innovative sector is responsible for more than a quarter of the total European R&D effort and plays a key role in the creation of economic growth and jobs throughout the economy. More and more Europeans live in a truly information-based society where the use of ICTs has rapidly accelerated as a core function of human social and economic interaction. According to Eurostat, 89% of EU enterprises actively used the Internet in 2004 and around 50% of consumers had recently used the Internet[12].

A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line.

In addition, because of increased connectivity between networks, other critical infrastructures (like transport, energy, etc.) are also becoming more and more dependent on the integrity of their respective information systems.

Both business and citizens in Europe still underestimate the risks. This is for various reasons, but the most important seems to be, in the case of enterprises, the poor visibility of the return on investment in security and, in the case of citizens, the fact that they are not aware of their responsibility in the global security chain.

Indeed, given the ubiquity of ICTs and information systems, network and information security is a challenge for everybody:

---

11 Radio Frequency Identification.

12 Eurostat, *Internet activities in the European Union*, 40/2005.

- **Public administrations** need to address the security of their systems, not just to protect public sector information, but also to serve as an example of best practice for other players.

- **Enterprises** need to address NIS more as an asset and an element of competitive advantage than as a "negative cost".

- **Individual users** need to understand that their home systems are critical for the overall "security chain".

In order to successfully tackle the problems described above, all stakeholders need reliable data on information security incidents and trends. However, reliable and comprehensive data on such incidents are difficult to obtain for many reasons, ranging from the rapidity with which security events can happen to the unwillingness of some organisations to disclose and publicise security breaches. Nonetheless, one of the cornerstones in developing a culture of security is **improving our knowledge of the problem**.

It is important that awareness programmes, designed to highlight security threats, do not undermine the trust and confidence of consumers and users by focusing only on negative aspects of security. Wherever possible, therefore, **NIS should be presented as a virtue and an opportunity** rather than as a liability and a cost. It needs to be viewed as an asset in building trust and consumer confidence, a competitive advantage for enterprises operating information systems, and a service quality issue for both public and private sector service providers.

The key challenge for policy makers is to achieve a holistic approach. This approach must recognise the respective roles of the various stakeholders. It must ensure proper coordination of the range of public policy and regulatory provisions that impact either directly or indirectly on NIS. The processes of liberalisation, deregulation and convergence have produced a multiplicity of players among the various stakeholder groups, which does not make this task easier. The contribution of ENISA to this goal can be important. ENISA could serve as a centre for information sharing, cooperation amongst all stakeholders, and the exchange of commendable practices, both within Europe and with the rest of the world, in order to contribute to the competitiveness of our ICT industries and a well-functioning Internal Market.

3. TOWARDS A DYNAMIC APPROACH TO A SECURE INFORMATION SOCIETY

A secure Information Society must be based on **enhanced NIS** and a widespread **culture of security**. To this end, the European Commission proposes a **dynamic and integrated approach** that involves all stakeholders and is based **on dialogue, partnership and empowerment**. Given the complementary roles of public and private sectors in creating a culture of security, policy initiatives in this field must be based on an **open and inclusive multi-stakeholder dialogue**.

This approach, and its associated actions, will complement and enrich the Commission's plan to continue the development of a comprehensive and dynamic policy framework through a number of initiatives in 2006:

(1) Addressing the evolution of spam and threats, like spyware and other forms of malware, in a Communication on these specific issues.

(2) Making proposals for improving cooperation between law enforcement authorities and addressing new forms of criminal activity that exploit the Internet and undermine the operation of critical infrastructures. This will be the subject of a specific Communication on cybercrime.

These policy initiatives also complement the activity being planned to achieve the goals of the Commission's Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP)[13], developed in response to a request by the December 2004 Council. The Green Paper process is likely to lead to an action plan combining an overall "umbrella" approach to critical infrastructure protection with the necessary sector-specific policies, including one for the ICT sector. The sector-specific policy for the ICT sector would examine, via **a multi-stakeholder dialogue**, the relevant economic, business and societal drivers with a view to enhancing the security and the resilience of networks and information systems.

Moreover, the 2006 review of the regulatory framework for electronic communications will also consider elements to improve NIS, such as 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.

It is largely up to the private sector to deliver solutions, services and security products to end users. It is therefore of strategic importance that **European industry be both a demanding user** of security products and services **as well as a competitive supplier** of NIS products and services.

National governments need to be able to identify and implement best practice in policy-making, as well as demonstrate commitment to these policy objectives by managing their own information systems in a secure manner. Public authorities, in Member States and at EU level, have a key role to play in properly informing users to enable them to contribute to their own security and safety. Raising awareness on NIS issues and providing appropriate and timely information via dedicated e-security web portals on threats, risks and alerts as well as on best practices should be priorities. To this end, examining the feasibility of **creating a European multilingual information sharing and alert system**, which would build upon and link together existing or planned national public and private initiatives, could be a major goal for ENISA.

The global dimension of network and information security challenges the Commission, both at international level and in coordination with Member States, to increase its efforts to **promote global cooperation on NIS**, notably in implementing the agenda adopted at the World Summit on the Information Society (WSIS) in November 2005.

Lastly, research and development, notably at EU level, will help develop new and innovative partnerships to boost the growth of the European ICT industry at large, and the European ICT security industry in particular. The Commission will therefore seek to ensure that appropriate financial resources are allocated to research on NIS and dependability technologies under the 7th EU Framework Programmes.

---

[13] COM(2005) 576, 17.11.2005.

3.1. Dialogue

3.1.1. As a first step to enhancing dialogue between public authorities, the Commission proposes initiating an exercise to **benchmark national NIS-related policies**, including specific security policies for the public sector. This exercise will help identify the most effective practices, so that they can then be deployed wherever possible on a broader basis throughout the EU and help make public administrations a driver of best practice in security. The work on electronic identification, for example as part of the recent eGovernment Action Plan, could play an important role in that respect.

If appropriately structured, the results of such a benchmarking exercise will **identify best practices to improve awareness among SMEs and citizens of the need** to address their own specific NIS challenges and requirements as well as their ability to do so. ENISA should be called upon to play an active role in this dialogue, and in consolidating and exchanging best practices.

3.1.2. A **structured multi-stakeholder debate** on how best to exploit existing tools and regulatory instruments to attain an appropriate societal balance between security and the protection of fundamental rights, including privacy, is needed. The planned Conference "i2010 – Towards a Ubiquitous European Information Society" being organised by the forthcoming Finnish Presidency, and the consultation on the security and privacy implications of RFID, which is part of the broader consultation recently launched by the Commission, will contribute to this debate. In addition, the Commission will organise:

- A business event to stimulate industry commitment to adopting effective approaches to implement a culture of security **in industry**.

- A seminar reflecting on ways to raise security awareness and strengthen the trust of **end-users** in the use of electronic networks and information systems.

3.2. Partnership

3.2.1. Effective policy making needs a clear understanding of the nature and extent of the challenges. This calls for not only reliable and up-to-date statistical and economic data both on information security incidents and levels of consumer and user confidence, but also up-to-date data on the size and trends of the ICT security industry in Europe. The Commission intends to ask ENISA to develop **a trusted partnership with Member States and stakeholders** to develop an **appropriate data collection framework**, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence.

In parallel, because of the highly fragmented market in the EU and its rather specific nature, the Commission will invite Member States, the private sector and the research community to **establish a strategic partnership** to ensure the availability of data on the ICT security industry and on the evolving market trends for products and services in the EU.

3.2.2. In order to improve the European capability to respond to network security threats, the Commission will ask ENISA to examine the **feasibility of a European**

information sharing and alert system to facilitate effective responses to existing and emerging threats to electronic networks. A requirement of such a system will be **a multilingual EU portal** to provide tailored information on threats, risks and alerts.

3.3. Empowerment

The empowerment of each stakeholder group is a prerequisite to foster awareness of security needs and risks in order to promote NIS.

3.3.1. In this respect the Commission invites **Member States** to:

- proactively participate in the proposed benchmarking exercise of national NIS policies;
- promote, in close cooperation with ENISA, awareness campaigns on the virtues, benefits and rewards of adopting effective security technologies, practices and behaviour;
- leverage the roll-out of e-government services to communicate and promote good security practices that could then be extended to other sectors;
- stimulate the development of network and information security programmes as part of higher education curricula.

3.3.2. The Commission also invites **private sector** stakeholders to take initiatives to:

- develop an appropriate definition of responsibilities for software producers and Internet service providers in relation to the provision of adequate and auditable levels of security. Here, support for standardised processes that would meet commonly agreed security standards and best practice rules is needed;
- promote diversity, openness, interoperability, usability and competition as key drivers for security as well as stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy-intrusive attacks;
- disseminate good security practices for network operators, service providers and SMEs as baseline levels for security and business continuity;
- promote training programmes in the business sector, in particular for SMEs, to provide employees with the knowledge and skills necessary to effectively implement security practices;
- work towards affordable security certification schemes for products, processes and services that will address EU-specific needs (in particular with respect to privacy);
- involve the insurance sector in developing appropriate risk management tools and methods to tackle ICT-related risks and foster a culture of risk management in organisations and business (in particular in SMEs).

4. CONCLUSIONS

Identifying and meeting security challenges in relation to information systems and networks in the EU requires the full commitment of all stakeholders. The policy approach outlined in this Communication seeks to achieve this by reinforcing **a multi-stakeholder approach**. This would build on mutual interests, identify respective roles and develop a dynamic framework to promote effective public policy-making and private sector initiatives.

The Commission will report to Council and Parliament in the middle of 2007 on the activities launched, the initial findings and the state of play of individual initiatives, including those of ENISA and those taken at Member State level and in the private sector. If appropriate, the Commission will propose a Recommendation on network and information security (NIS).