European Economic and Social Committee

TEN/254
Secure Information Society

Brussels, 16 February 2007

OPINION

of the
European Economic and Social Committee
on the
Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – A strategy for a Secure Information Society – Dialogue, partnership and empowerment
COM(2006) 251 final

_____

99 rue Belliard - B-1040 Brussels - Tel. +32 (0)2 546 90 11 - Fax +32 (0)2 513 48 93 - Internet http://www.eesc.europa.eu

EN

On 31 May 2006 the Commission decided to consult the European Economic and Social Committee, under Article 262 of the Treaty establishing the European Community, on the

> *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – A strategy for a Secure Information Society – Dialogue, partnership and empowerment*
> COM(2006) 251 final.

The Section for Transport, Energy, Infrastructure and the Information Society, which was responsible for preparing the Committee's work on the subject, adopted its opinion on 11 January 2007. The rapporteur was Mr Pezzini.

At its 433rd plenary session, held on 15-16 February 2007 (meeting of 16 February), the European Economic and Social Committee adopted the following opinion by 132 votes, nem. con. with two abstentions.

*

* *

1. Conclusions and recommendations

1.1 The EESC firmly believes that information security is of growing concern for businesses, administrations, public and private bodies and individuals.

1.2 In general, the EESC agrees with the analyses and considerations calling for a new strategy, to increase network and information security against attacks and intrusion, which have no geographical boundaries.

1.3 The EESC believes that the Commission should make further endeavours to achieve an innovative, coordinated strategy, given the scale of the issue and its economic implications and impact on privacy.

1.3.1 Moreover, the EESC points out that the Commission has recently adopted a new Communication on information security and that another document is due to be issued in the near future on the same subject. The EESC reserves the right to issue a more comprehensive Opinion in the future which takes all the Communications into account.

1.4 The EESC stresses that the issue of information security cannot in any way be separated from the need to increase protection of personal data and to protect freedoms, as safeguarded by the European Convention on Human Rights.

1.5 The EESC wonders, as things stand, what the proposal's added value is over the integrated approach adopted in 2001, whose aim was the same as that specified in this Communication[1].

1.5.1 The Impact Assessment[2] appended to the proposal is an improvement on the 2001 position in a number of respects, but it has only been published in one language and is therefore inaccessible to many European citizens, who form their opinion from the official document, which is in the Community languages.

1.6 The EESC draws attention to the conclusions of the 2005 Tunis World Summit relating to the information society, endorsed by the UN Assembly of 27 March 2006:

- principles of non-discrimination regarding access;
- promotion of ICTs as a tool for peace;
- instruments to enhance democracy, cohesion and good governance;
- prevention of abuse, with due regard for human rights[3].

1.7 The EESC stresses that a dynamic, integrated Community strategy should tackle, in addition to dialogue, partnership and responsibility:

- prevention measures;
- the need to move beyond information security to information assurance[4];
- provision of a clear, recognised EU framework of laws, regulations and penalties;
- strengthening of technical standardisation;
- digital identification of users;
- launching of European foresight exercises on information security, in conditions of multimodal technological convergence;
- strengthening of European and national risk-assessment mechanisms;
- measures to avoid the emergence of information monocultures;
- increased Community coordination at European and international level;
- setting up of an ICT Security Focal Point between Directorates-General;
- creation of a European Network and Information Security Network;
- optimisation of the role of European research into information security;
- launch of a "European Secure Computer Day";

---

1 Cf. EESC Opinion on the *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on network and information security: Proposal for a European policy approach* OJ C 48 of 21/2/2002 page 33.

2 The Impact Assessment does not carry as much weight as a strategy paper.

3 UN, 27.0306, Recommendations Nos 57 and 58. Tunis Final Document No 15.

4 Cf. Emerging strategies in the context of security, JRC – Institute for the Protection and Security of the Citizen, strategic research dossier, September 2005, European Commission, http://serac.jrc.it.

- Community pilot measures in schools of various kinds and levels, on information security issues.

1.8 Lastly, the EESC believes that in order to ensure a dynamic, integrated Community strategy, relevant budgetary appropriations need to be allocated and enhanced-cooperation initiatives and measures planned at Community level which can present Europe to the world with a unified voice.

2. Reasons

2.1 Security in the information society is a fundamental issue in terms of ensuring reliable communication networks and services inspiring confidence, which are key factors in economic and social development.

2.2 Information networks and systems need to be protected to preserve competitive and trade capacities, ensure the integrity and continuity of electronic communications, prevent fraud and guarantee protection of privacy by the law.

2.3 Electronic communications and related services are the largest segment in the entire telecommunications sector: in 2004 approximately 90% of European businesses actively used the Internet, with 65% of them creating their own website, while an estimated 50% of European people regularly use the Internet and 25% of households use broadband access on an ongoing basis[5].

2.4 Despite faster investment growth, only 5-13% of total investment in information technologies is spent on security. This is too little. Recent studies have revealed that out of an average of 30 protocols that share key structures, 23 are vulnerable to multi-protocol attacks[6]. In addition, on average, an estimated 25 million spam[7] emails are sent every day and so the EESC welcomes the Commission's recent proposal on the subject.

---

5 i2010: a strategy for a secure information society – Factsheet 8 (June 2006), EC Information Society and Media http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

6 Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) - Volume 00 ARES 2006 Publisher**:** IEEE Computer Society.

7 SPAM = Unsolicited commercial email. The original meaning of spam is "spiced pork and ham" and describes canned meat which was very popular during World War II when it became the primary source of food for the US troops as well as the residents of the United Kingdom. After years of eating spam, as it was not rationed, people were fed up with it.

2.5 As regards computer viruses[8], worms[9] and spyware[10] have mushroomed with the increasingly rapid development of electronic communication networks and systems, which have become increasingly complex and, at the same time, vulnerable, thanks, not least, to the convergence of multimedia, mobile telephony and GRID infoware[11]: extortion, DDoS (distributed denial of service), Internet ID theft, phishing[12], piracy[13] etc. are security problems for the information society, which the European Community addressed in a Communication in 2001[14]. The EESC commented on the Communication[15], identifying three lines of action:

– specific security measures;
– legal framework, including the protection of data and privacy;
– combating cyber-crime.

2.6 Finding adequate solutions is a challenge when it comes to recording, identifying and preventing information attacks concerning a network system, given the constant configuration changes, the variety of network protocols and services provided and developed and the extremely complex, asynchronous nature of attacks[16].

2.7 Regrettably, however, the poor visibility of the return on investments in security and the fact that few users assume responsibility have resulted in risks being underestimated and little focus on developing a security culture.

---

8 *Computer virus*: specific software belonging to the malware category which, once executed, can infect files so that they reproduce, making copies of themselves, usually without discovery by the user. Viruses can cause varying degrees of damage to the host operating system and, at the very least, result in resources being wasted in terms of RAM, CPU and hard disk space. (www.wikipedia.org/wiki/virus_informatico).

9 Worm = self propagating malware: an email worm is a disruptive network attack that collects all email addresses from a client email programme (e.g. MS Outlook) and then sends hundreds of emails to those email addresses with the worm programme itself as an attachment.

10 Spyware = software programmes that track a user's Internet surfing, which install themselves without informing the user and without their knowledge, authorisation or control.

11 GRID infoware = enables the sharing, selection, and aggregation of a wide variety of geographically distributed computational resources (such as supercomputers, compute clusters, storage systems, data sources, instruments, people) and presents them as a single, unified resource for large-scale computing and data intensive computing applications.

12 Phishing = in information technology, a cracking technique used to gain access to personal and confidential data for the purpose of ID theft by means of fake emails created in such a way as to appear genuine.

13 Piracy = a term used by software "pirates" to describe software that has been stripped of its copy-protection and made available on the Internet for downloading.

14 COM(2001) 298 final.

15 See footnote 1.

16 Multivariate Statistical Analysis for Network Attacks Detection. Guangzhi Qu, Salim Hariri* - 2005 US, Arizona Internet Technology Laboratory, ECE Department, The University of Arizona, http://www.ece.arizona.edu/~hpdc Mazin Yousif, Intel Corporation, USA. - Work supported in part by a grant from Intel Corporation IT R&D Council.

3. The Commission proposal

3.1 The Commission's Communication on a Strategy for a Secure Information Society[17] attempts to improve information security through a dynamic, integrated strategy based on:

a) enhancing dialogue between public authorities and the Commission, benchmarking national policies and identifying best electronic communication practices in the field of security;
b) more campaigns to raise awareness among the public and SMEs of the need for effective security systems. The Commission should promote these campaigns and the European Network and Information Security Agency (ENISA) should be more involved;
c) dialogue on instruments and rules to achieve a balanced relationship between security and fundamental rights, including the protection of privacy.

3.2 Furthermore, the Communication envisages a trusted partnership with ENISA to develop a suitable framework for collecting data on breaches of security, user confidence and developments in the security industry:

a) with Member States;
b) with consumers and users;
c) with the information security industry;
d) with the private sector,

setting up a multilingual EU information and risk alert portal, with a view to a strategic partnership between the private sector, Member States and researchers.

3.2.1 The Communication also provides for greater empowerment of stakeholders with regard to security needs and risks.

3.2.2 As regards international cooperation with third countries, the Commission states that "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"[18]. However, this recommendation is not reflected in the dialogue, partnership and empowerment actions.

17 COM(2006) 251 of 31.05.06.

18 Cf. COM(2006) 251, penultimate paragraph of chapter 3.

4. Comments

4.1 The EESC agrees with the analyses and arguments in favour of a dynamic, integrated European strategy for secure networks and information; it believes that the issue of security is essential to fostering a more favourable attitude towards using information technologies, and to boosting trust in them. The EESC's views have been stressed in numerous opinions[19].

4.1.1 The EESC reiterates[20] that: "… the Internet and new technologies for online communication (for example, mobile telephones and palmtop computers with Internet and multimedia functions, currently undergoing rapid growth) are of fundamental importance for the development of the knowledge economy, the *e*economy and *e*government."

4.2 Strengthening the Commission's proposals

4.2.1 The Commission proposes to base this dynamic, integrated strategy on an open, inclusive multi-stakeholder dialogue which includes users in particular, together with enhanced partnership and empowerment. The EESC feels that the approach could be made even wider.

4.2.2 This view has been stressed in previous opinions: " … to be effective, this programme should directly involve all Internet users, who need to be trained and informed of the precautions to take and the resources to use in order to protect themselves from being sent harmful or unwanted content, or from being used to forward such content. In the view of the EESC, one of the priorities of the action plan in regard to information and training should be to gain the support of users …."[21].

4.2.3 However, the EESC feels that users' and citizens' support must be gained in such a way as to reconcile the necessary protection of information and networks with civil liberties and users' right to secure, reasonably-priced access.

19
- See EESC opinion on the *Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* - OJ C 69 of 21/3/2006 page 16*;*
- EESC opinion on the *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on i2010 – A European Information Society for growth and employment* – OJ C 110 of 9/5/2006 page 83;
- EESC opinion on the *Proposal for a Decision of the European Parliament and of the Council on establishing a multi-annual Community programme on promoting safer use of the Internet and new online technologies* – OJ C 157 of 28/6/2005 page 136;
- EESC opinion on the *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on network and information security: proposal for a European policy approach* – OJ C 48 of 21/2/2002 page 33.

20 See footnote 19, third bullet point.

21 See footnote 19, third bullet point.

4.2.4 It should be borne in mind that information security entails cost for the consumer, not least in terms of the time wasted in removing or circumnavigating obstacles. The EESC believes that a requirement should be introduced for automatic bundling of anti-virus software with every computer; the user could decide whether or not to activate it but it would be included in the product at manufacture.

4.3 **Towards a more dynamic, innovative Community strategy**

4.3.1 In addition to this, the EESC feels that the EU should set itself more ambitious goals and launch an innovative, integrated, dynamic strategy with new initiatives such as:

- Mechanisms allowing digital identification of individual users, who are too often asked to give their personal data.

- Measures implemented through ETSI[22], necessary to ensure secure use of ITCs, providing rapid ad-hoc solutions, defined as a common security threshold throughout the EU.

- Prevention measures incorporating minimum security requirements into information and network systems, and the launch of pilot measures in the form of courses on security in schools of all kinds and levels.

- Setting-up at European level of a clear, recognised legal and regulatory framework. Applied to information technology and networks, this framework would make it possible to move beyond information security to information assurance.

- Strengthening of European and national risk-assessment measures and greater ability to implement laws and regulations, to crack down on information crimes attacking privacy and data archives.

- Measures to avoid the emergence of information monocultures with products and solutions that are more easily pirated. Support for new, diversified multicultural innovations with a view to the creation of a Single European Information Space (SEIS).

22 ETSI, European Telecommunications Standards Institute, cf. in particular the Workshop of 16-17 January 2006. ETSI has drawn up, *inter alia*, specifications on unlawful interception (TS 102 232; 102 233; 102 234), Wireless Lan Internet access (TR 102 519) and electronic signatures, and has developed security algorithms for GSM, GPRS and UMTS.

4.3.2 The EESC advocates the creation of an inter-DG ICT-Security Focal Point[23]. The Focal Point would allow action:

- within the Commission;
- at the level of the individual Member States, by means of horizontal solutions for interoperability, identity management, protection of privacy, freedom of access to information and services, and minimum security requirements;
- at international level, to ensure a unified European voice in different contexts such as the UN, G8, OECD, ISO.

4.4 **Towards enhanced responsible-coordination measures at EU level**

4.4.1 The EESC also attaches great importance to the creation of a European Network and Information Security Network, which could act as a channel for the promotion of surveys, research and workshops on security mechanisms and the interoperability thereof, advanced cryptography and the protection of privacy.

4.4.2 The EESC believes that the role of European research in this very sensitive sector would be optimised by a useful synthesis of the provisions of:

- the European Security Research Programme (ESRP)[24] included in the 7th RTD Framework Programme;
- the Safer Internet Plus Programme;
- the European Programme for Critical Infrastructure Protection (EPCIP)[25].

4.4.3 Another suggestion is to launch a "European Secure Computer Day", supported by national education campaigns in schools and information campaigns targeting consumers, on IT information protection procedures. This would, of course, be in addition to information on the technological progress made in the huge, ever-changing field of computers.

4.4.4 The EESC has pointed out on a number of occasions that "The perceived security of and trust in digital transactions determines the speed with which enterprises are likely to exploit ICT in their business. Consumers' willingness to provide credit card numbers on a web page is greatly influenced by the perceived safety of the action"[26].

---

23 This inter-DG Focal Point could be financed under the IST Priority of the FP7 – RTD Cooperation Programme, or by the European Security Research Programme (ESRP).

24 Cf. EU FP7 – RTD Framework Programme, Cooperation Programme; Security Research Thematic Priority with a budget of EUR 1.35 billion for the 2007-2013 period.

25 COM(2005) 576 of 17.11.2005.

26 See footnote 19, second bullet point.

4.4.5 The EESC firmly believes that, given the sector's huge growth potential, specific policies must be introduced and existing policies brought into line with new developments. An integrated information security strategy linking European initiatives is needed, breaking down the borders between sectors and ensuring uniform, secure dissemination of ICTs throughout society.

4.4.6 In the EESC's view, a number of major strategies, including the one in question, are progressing too slowly because of bureaucratic and cultural hindrances, introduced by Member States, to the essential decisions which have to be taken at Community level.

4.4.7 The EESC also believes that Community resources are insufficient to achieve numerous, urgent projects which can only provide practical responses to the new challenges of globalisation if implemented at Community level.

4.5 **Towards a greater EU guarantee of consumer protection**

4.5.1 The EESC is aware that the technological security measures and security management procedures introduced by Member States are geared to their individual needs and tend to focus on different aspects. That is another reason why it is difficult to provide a single, effective response to security issues. With the exception of some administrative networks, there is no systematic cross-border cooperation between Member States, despite the fact that security issues cannot be addressed by each individual country on its own.

4.5.2 The EESC notes, moreover, that Council Framework Decision 2005/222/JHA introduced a framework for cooperation between judicial and other competent authorities to ensure, by approximating Member States' criminal law on attacks against information systems, that their approaches are coherent in the following areas:

- illegal access to information systems;
- illegal system interference, i.e. intentional serious hindering or interruption of the functioning of an information system;
- illegal data interference, i.e. the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system;
- instigation, aiding and abetting with regard to the above offences.

4.5.3 The Framework Decision also lays down criteria for establishing the liability of legal persons and any penalties that may be applied once their liability has been ascertained.

4.5.4 As regards dialogue with Member States' public authorities, the EESC supports the Commission's proposal that these authorities should initiate an exercise to benchmark national

NIS-related policies, including specific policies for the public sector. This suggestion was made in an EESC Opinion in 2001[27].

4.6 **Towards a more widespread security culture**

4.6.1 With regard to involvement of the information security industry, the industry must protect its customers' right to privacy and confidentiality by providing effective guarantees that the tools used for the material surveillance of their installations – and for commercial encryption – are in line with technological developments[28].

4.6.2 As regards awareness-raising campaigns, the EESC believes that a genuine "security culture" must be created, in such a way as to be fully compatible with freedom of information, communication and expression. Numerous users are unaware of all the risks related to computer piracy, while many service providers, sellers and operators are unable to assess the existence and extent of vulnerable aspects.

4.6.3 Although the main aim is to protect privacy and personal data, consumers also have the right to genuinely effective protection against improper personal profiling by spyware and web bugs, or other means. Effective measures are also needed to curb spamming[29] (mass sending of unsolicited mail) which often also arises out of such misuse. Intrusion of this kind is damaging to those concerned[30].

4.7 **Towards a stronger, more active EU Agency**

4.7.1 The EESC is in favour of a greater, more effective role for the European Network and Information Security Agency (ENISA), as regards both awareness-raising campaigns and, most importantly, information and training schemes for operators and users. This has already been recommended by the EESC in a recent opinion[31] on the provision of public electronic communication services.

4.7.2 Lastly, as regards the proposed initiatives to empower each stakeholder group, these appear to entail strict observance of the subsidiarity principle. Indeed, they are to be the responsibility of the Member States and the private sector, in accordance with their specific remits.

---

27 See footnote 19, fourth bullet point.

28 See Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24 of 30.01.1998).

29 *Pollupostage*, in French.

30 See EESC opinions on (i) electronic communications networks (OJ C 123 of 25.4.2001 p. 50), (ii) electronic commerce (OJ C 169 of 16.6.1999, p. 36) and (iii) the effects of e-commerce on the single market (OJ C 123 of 25.4.2001, p.1).

31 See footnote 19, first bullet point.

4.7.3 ENISA should be able to use contributions from the European Network and Information Security Network to organise joint activities, as well as the multilingual Community information-security alert web portal for personalised, interactive, user-friendly information targeted particularly at individual users of all ages and small and medium-sized businesses.

Brussels, 16 February 2007.

The President of the European Economic and Social Committee	The Secretary-General of the European Economic and Social Committee
Dimitris Dimitriadis	Patrick Venturini