Opinion of the Committee of the Regions on the 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for a European Policy Approach'

(2002/C 107/27)

THE COMMITTEE OF THE REGIONS,

having regard to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions — Network and Information Security: Proposal for a European Policy Approach (COM(2001) 298 final);

having regard to the decision of the Commission of 7 June 2001, under the first paragraph of Article 265 of the Treaty establishing the European Community, to consult it on the subject;

having regard to the decision of the president of the Committee of the Regions of 2 July 2001 to instruct Commission 3 — Trans-European Networks, Transport and the Information Society to draw up the relevant opinion;

having regard to the decision of its President of 26 October 2001 to appoint Ms Barrero Flórez as rapporteur-general for its opinion, under Rule 40(2) of its Rules of Procedure;

having regard to its opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — Creating a safer information society by improving the security of information infrastructures and combating computer-related crime: eEurope 2002 (COM(2000) 890 final — CdR 88/2001 fin);

having regard to the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — Ensuring security and trust in electronic communication: Towards a European framework for digital signatures and encryption (COM(97) 503 final);

having regard to the Communication from the Commission to the Council and the European Parliament — eEurope 2002: Impact and priorities (COM(2001) 140 final);

having regard to the eEurope 2002 Action Plan (COM(2000) 330 final);

having regard to the Draft Convention on Cyber-crime of the Council of Europe (COM(2001) 103);

having regard to the Council Recommendation on common information technology security evaluation criteria ([1]);

having regard to the Council Recommendation on contact points maintaining a 24-hour service for combating high-tech crime ([2]);

having regard to Regulation (EC) No 45/2001 of the European Parliament and Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ([3]);

having regard to Council Resolution No 9194/01 of 20 June 2001 on law enforcement operational needs with respect to public telecommunication networks and services;

having regard to the Presidency Conclusions of the Stockholm European Council of March 2001;

having regard to Directive 90/388/EC on competition in the markets for telecommunications services;

([1]) OJ L 93, 26.4.1995.
([2]) OJ C 187, 3.7.2001.
([3]) OJ L 8, 12.1.2001.

having regard to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

having regard to Directive 97/33/EC on interconnection with telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (ONP);

having regard to Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector;

having regard to Directive 98/10/EC on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment;

having regard to Directive 1999/93/EC on a Community framework for electronic signatures;

having regard to Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce);

having regard to the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector [1];

having regard to the draft opinion (CdR 257/2001 rev.) drawn up by the rapporteur-general, Ms Barrero Flórez (E-PES, Director-General for European Affairs, Government of the Principality of Asturias);

whereas:

— information networks and systems have become a key factor in present-day economic and societal development, and their proper availability is crucial to vital infrastructures such as energy supply and road transport, as well as most public and private services and the economy as a whole;

— the security of information networks and systems is becoming a prerequisite for the future development of new services, new sources of economic wealth, innovative commercial links, etc.;

— user confidence in information networks is seriously jeopardised by the growing number of breaches of network security;

— the lack of confidence in information networks and systems is slowing down the widespread introduction of new services connected with the information and knowledge society;

— the security of these networks and systems has become a key challenge for policy makers, who must be aware of their importance and have an understanding of the different aspects involved, the underlying security issues at stake and their role in improving security;

— a substantial body of legislation as part of the telecommunications framework and personal data protection law have been put in place, but no specific security-related measures have yet been adopted;

— many problems remain unsolved and solutions are slow coming to the market as a result of certain market imperfections;

— the public authorities have a part to play in remedying market failings or shortcomings;

---

[1] OJ C 365, 19.12.2000.

— specific policy measures addressing these imperfections which affect information networks and systems can reinforce the market process and at the same time improve the functioning of the legal framework;

— such measures must be part of a European approach in order to ensure the development of the information and knowledge society in the European Union, to benefit from common solutions, and to be able to act effectively at global level;

— the complex nature of the problem means that its political, economic, organisational and technical aspects must be taken into account, together with its decentralised and global character;

— the effects of the lack of information system and network security in the less developed regions of Europe may widen the digital gap between them and the most developed and secure regions;

— regional and local authorities can and must play a key role in implementing a European information system and network security policy, since with their proximity to citizens, organisations and businesses they are ideally placed to apply whatever practical measures are decided with the necessary effectiveness,

adopted the following opinion unanimously at its 41st plenary session of 14 and 15 November 2001 (meeting of 15 November).

Introduction

The Committee of the Regions

1. shares the Commission's growing concern regarding the security of networks and information systems and agrees that it is of critical importance not only for the development of the information and knowledge society but also for today's world economic system;

2. agrees with the communication regarding the political priority which the European Union must give to information systems and network security. The market has been unable to provide a unified response because of the existence of multiple technologies and security standards, without an accepted, open standard common to all;

3. endorses the objective of the communication, which is to identify where additional or enhanced public action at European or national level is required in order to forge a Community network and information security policy;

4. is concerned regarding respect for the freedoms and civil rights acknowledged by the Universal Declaration of Human Rights, the International Convention on Civil and Political Rights and the European Convention on Human Rights in connection with the measures to be adopted to increase the security of networks and information systems. To this end, it calls for clear limits to be set to any powers or capacities which could result in civil liberties being jeopardised. The Committee of the Regions is convinced that a balance between respect for freedoms and civil rights on the one hand, and network and information system security on the other, is possible;

5. in view of the cross-border nature of the problem, doubts if this concerted Community-level policy can achieve its aims without the agreement of international organisations and other world powers;

6. urges the Commission to accelerate the implementation of any practical measures adopted and provide sufficient economic resources, in order to meet the important and urgent need to ensure the security of networks and information systems;

Analysis of network and information security issues

The Committee of the Regions

7. considers that the definition of network and information security given in the communication, 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' to be unclear in its reference to 'a given level of confidence'. The Committee of the Regions believes that no malicious action or intrusion of a network or information system is acceptable, at any 'level of confidence';

8. is extremely concerned to note that investment in security is neither a priority issue nor on an appropriate scale among most of the telecommunications service and access providers operating in Europe. Moreover, the presence of small regional operators whose priority is to secure an economically viable market position, leading them to overlook security, is a further difficulty and a factor which must be considered;

9. is convinced that confidence in encryption products will largely flow from the introduction of open international standards, and considers the uncoordinated efforts by a number of Member States to support open source encryption software to be unproductive, given the powerful and unstoppable negotiating initiative of the private sector;

10. agrees with the communication that competition amongst hardware and software vendors is not producing greater investment in security, and therefore proposes that means of encouraging such investment be examined;

11. considers that telecommunications operators and access providers must be obliged to meet a series of minimum security requirements, which should be determined at Community level.

A European policy approach

The Committee of the Regions

12. considers that the balanced development of the information and knowledge society in the European Union will facilitate cohesion and the construction of a Europe of the regions, and that it is therefore essential to guarantee the security of networks and information systems;

13. agrees with the communication from the Commission regarding the social benefits generated by any investment in improved network and information system security, and would point to the high cost in terms of social well-being incurred by the failure by manufacturers, operators and service providers to make such investment;

14. urges the Commission to examine the need to set mandatory security criteria and standards to be met by all information systems deemed to be basic (services of general interest) which are connected to telecommunications networks and internal networks;

15. advocates maximising security without compromising the easy, high-quality access underpinning the information and knowledge society, but considers it essential to maintain minimum levels of security even if this impairs quality of access;

16. agrees with the communication that:

— a common understanding is needed of the underlying security issues and the specific measures to be taken;

— policy measures can reinforce the market process and at the same time improve the functioning of the legal framework;

— a European policy approach is needed to ensure an internal market for such services, to benefit from common solutions, and to be able to act effectively on a global level;

17. argues that the awareness-raising actions proposed in the communication should be backed up with support or assistance for investment in security measures, so that measures acknowledged to be necessary are not delayed on the grounds of economic cost;

18. emphasises the importance, for operational and practical reasons, of regional and local administrations playing a prominent part in any awareness-raising campaigns launched in this area;

19. endorses the communication's proposal to strengthen the CERT system in the European Union as a matter of urgency, and to equip existing centres with sufficient human, technical and economic resources;

20. recommends a more intensive, direct and flexible relationship between European CERTs and potential final beneficiaries;

21. endorses the communication's proposals for action on a European warning and information system, and at the same time suggests proactive measures such as setting up a European Network and Information Systems Security Agency. The agency's functions would include analysing and testing all software (operating systems, navigators, e-mail managers, etc.) to be used in public information networks, in order to detect security 'loopholes' in software not yet marketed n the European Union. The Committee of the Regions does not view the future institute for the protection and security of citizens under the aegis of the Joint Research Centre (JRC) as matching the agency it advocates in either stature or functions;

22. fears that any research into network and information security funded by the Community's framework R&D programmes which is not supported by the main software manufacturers on the market will not obtain the hoped-for concrete results. The Committee of the Regions proposes that efforts be made independently to secure a great commitment on the part of the main world software manufacturers to research on network and information safety and its immediate practical application;

23. expresses its concern at the current absence of interoperability between the various technological solutions offered by manufacturers and their lack of interest in devising shared open standards;

24. advises against encouraging the use of particular solutions or encryption products when what should be sought is for all solutions to fit a common open standard, accepted by all manufacturers;

25. considers it vital to forge agreements between the various European certification service providers regarding mutual recognition of certificates. Without such an agreement, the usefulness of electronic certificates will be severely limited, and use will not reach the desired level. Setting up regional authorities with non-interoperable systems as certification service providers gives ground for concern, as this most certainly complicates achieving the aim of a cohesive, well-structured Europe of the regions;

26. warmly welcomes the European Electronic Signatures Standardisation Initiative (EESSI), the smart card initiative in eEurope and the Public Key Infrastructure (PKI) initiatives;

27. agrees that harmonisation of specifications will lead to increased interoperability, at the same time enabling swift implementation by market players;

28. accepts all the proposed actions to provide support for market-oriented standardisation and certification, and believes that a legal initiative on mutual recognition of certificates should be mounted;

29. considers that there should be regular checks on the degree of implementation by telecommunications service operators of the technical and organisational measures to safeguard the security of their services, laid down in Article 4 of the Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector;

30. would alert the Commission to the potentially grave consequences of terrorist groups committing cyber-crimes designed to maximise damage to collective interests as a form of political blackmail;

31. agrees with all the proposed actions regarding the legal framework, and is convinced of the need for approximation and harmonisation of national legislation on cyber-crime so that no European country can serve as a refuge from which cyber-crime can go unpunished or incur lighter penalties;

32. proposes that the creation of specialist police cyber-crime units at national level be encouraged where they do not yet exist, and that existing units be coordinated. The necessary human and technical resources must also be made available;

33. recommends that special cyber-crime prosecutors, who have received thorough specialist training enabling them to carry forward public prosecutions with due efficacy, be appointed in all the Member States. Communication and coordination between the special prosecutors must be acknowledged as crucial, as must relevant training for judges, so that acts potentially endangering the security of networks and those having access to them can be efficiently pursued;

34. fully agrees with the Commission communication that the development of e-administration — on which many regional and local authorities are counting to enhance their links with citizens, the quality of their services and, in general, public welfare and democratic participation — makes public administrations both potential exemplars in demonstrating effective secure solutions and market actors with the ability to influence developments through their procurement decisions. Public administrations are therefore duty-bound to give an initial impetus to the information and knowledge society, within the limits of their remit. If the networks and information systems used by administrations are not secure, the public's lack of confidence in them will be highly prejudicial to the development of this new society;

35. proposes that actions concerning public administrations should be embrace the three administrative levels (local, regional and national), and that interoperability of the applied solutions should be an essential objective;

36. is strongly in favour of stepping up the dialogue with international organisations and partners on network security, and in particular on how to boost the security of electronic networks, and urges the Commission to consider organising a world summit on network and information system security, bringing in manufacturers and operators, as well as to set up a European forum for combating cyber-crime. It also calls upon the Member States to ratify the Council of Europe's recently approved final draft of an International Convention on Cyber-crime, so that the convention can come into force, and the legal instruments it contains be implemented, as soon as possible.

Brussels, 15 November 2001.

The President

of the Committee of the Regions

Jos CHABERT