EUROPEAN PARLIAMENT

1999 *2004*

Session document

FINAL
A5-0311/2002

17 September 2002

REPORT

on the Commission communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on 'Network and information security: proposal for a European policy approach'
(COM(2001) 298 – C5-0657/2001 – 2001/2280(COS))

Committee on Citizens' Freedoms and Rights, Justice and Home Affairs

Rapporteur: Elena Ornella Paciotti

CONTENTS

Page

PROCEDURAL PAGE

By letter of 7 June 2001, the Commission forwarded to Parliament a communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on 'Network and information security: proposal for a European policy approach' (COM(2001) 298 – 2001/2280(COS)).

At the sitting of 13 December 2001 the President of Parliament announced that she had referred the communication to the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs as the committee responsible and the Committee on Legal Affairs and the Internal Market, the Committee on Industry, External Trade, Research and Energy and the Committee on Culture, Youth, Education, the Media and Sport for their opinions (C5-0657/2001).

The Committee on Citizens' Freedoms and Rights, Justice and Home Affairs had appointed Elena Ornella Paciotti rapporteur at its meeting of 10 October 2001.

The committee considered the Commission communication and the draft report at its meetings of 23 May, 17 June, 8 July and 12 September 2002.

At the last meeting it adopted the motion for a resolution by 27 votes to 1, with 2 abstentions.

The following were present for the vote: Jorge Salvador Hernández Mollar, chairman; Robert J.E. Evans, vice-chairman; Giacomo Santini, vice-chairman; Elena Ornella Paciotti, rapporteur; Niall Andrews, Roberta Angelilli, Alima Boumediene-Thiery, Marco Cappato (for Mario Borghezio), Michael Cashman, Charlotte Cederschiöld, Ozan Ceyhun, Carlos Coelho, Gérard M.J. Deprez, Giuseppe Di Lello Finuoli, Adeline Hazan, Anna Karamanou (for Martin Schulz), Timothy Kirkhope, Eva Klamt, Alain Krivine (for Ole Krarup), Bill Newton Dunn, José Ribeiro e Castro, Martine Roure, Miet Smet (for Hubert Pirker), Patsy Sörensen, The Earl of Stockton (for The Lord Bethell), Joke Swiebel, Fodé Sylla, Anna Terrón i Cusí, Maurizio Turco, Christian Ulrik von Boetticher and Olga Zrihen Zaari (for Walter Veltroni).

The opinion of the Committee on Industry, External Trade, Research and Energy is attached; the Committee on Legal Affairs and the Internal Market decided on 27 November 2001 not to deliver an opinion; the Committee on Culture, Youth, Education, the Media and Sport decided on 21 November 2001 not to deliver an opinion.

The report was tabled on 17 September 2002.

MOTION FOR A RESOLUTION

European Parliament resolution on the Commission communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on 'Network and information security: proposal for a European policy approach' (COM(2001) 298 – C5-0657/2001 – 2001/2280(COS))

The European Parliament,

– having regard to the Commission communication (COM(2001) 298 – C5-0657/2001[1]),

– having regard to its recommendation of 6 September 2001 on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime and the Council of Europe Convention on Cybercrime, signed in Budapest on 26 November 2001[2],

– having regard to the proposal of 19 April 2002 for a Council Framework Decision on attacks against information systems which implements the relevant aspects of the aforementioned Council of Europe Convention (COM(2002) 173),

– having regard to the conclusions of the European Council meetings held in Stockholm in March 2001 and Seville on 21 and 22 June 2002 and the Commission communication entitled 'eEurope 2005: An information society for all', which draw attention to the urgent need to ensure network security,

– having regard to the other relevant resolutions on the subject, including its resolution of 5 September 2001 on the existence of a global system for intercepting private and commercial communications (ECHELON interception system) and the latest initiatives taken at international level (G8, OECD, UN)[3],

– having regard to Rule 47(1) of its Rules of Procedure,

– having regard to the report of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs and the opinion of the Committee on Industry, External Trade, Research and Energy (A5-0311/2000),

As regards the importance of secure networks in the information society

A. having regard to the rapid convergence of electronic communications networks which are increasingly becoming a key factor in economic and social terms,

B. whereas, as a result of this convergence, it is necessary to create an adequate policy and legal framework in the European Union to guarantee the protection of network

[1] OJ C 43, 16.2.2002. p. 2.
[2] Texts adopted (P5 TAPROV(2001)0284).
[3] Texts adopted (P5 TAPROV(2001)0264).

and information security, which is an essential precondition for existence of the Information Society,

C. considers an appropriate level of network security to be a key factor in the development of network services and electronic commerce and in the smooth operation of the internal market,

D. whereas measures to improve security can be effective only if all those concerned (public authorities, consumers, university researchers, businesses), including individual citizens, are aware of the security risks and their own responsibility regarding precautions to be taken,

E. whereas solutions to increase safety are effective only if they are applied by all the market players concerned, preferably on the basis of open international standards,

F. whereas the Computer Emergency Response Teams (CERTs) operate in different ways in different Member States, thereby unnecessarily complicating efforts to achieve cooperation,

1. Points out that the present level of security is inadequate, given that 60% of European businesses have already experienced serious problems over the last two years, that only 14% of them implement a network security policy and that a lack of security is the main obstacle to Internet use for 62% of SMEs and 81% of large companies[1];

2. Points out, furthermore, that users often appear unable to protect themselves against threats to network security, which include malicious attacks and unintentional events such as:

- the interception of ***both wired and wireless*** communications via ***SOTA electronic surveillance systems,*** routers, gateways and network servers; unauthorised access gained through password cracking or malicious misrepresentation;
- network disruption following server or router attacks, flooding or denial-of-service attacks or attacks on data integrity involving the execution of malign software, such as viruses, that modify or destroy data;
- environmental and unintentional events (such as natural disasters);
- criminal attacks, which in some cases may have a terrorist intent;

3. Notes the fact that network attacks may be targeted at essential infrastructure such as transport, communications, energy and water supply networks and financial and banking services, and that network vulnerability therefore carries with it serious risks for the smooth operation of the Union's economy and the daily lives of EU citizens;

4. Considers that any response to these weaknesses that is based solely on action taken on a voluntary basis by those directly concerned would be inadequate, owing to differences in approach, the lack of common standards and the swift pace of technological change; at the same time stresses that it is appropriate for producers to develop secure products and to

[1] ESTO 'Future bottlenecks in the information society', report to the EP, ITRE Committee, p. 143, and Eurostat.

participate in development in the field of product security;

5. Emphasises the need to ensure as soon as possible that all citizens, businesses and administrations have access to the public electronic services of all EU administrations via a secure and personalised authenticated access system; considers that in order to ensure this, electronic signatures should be used and European standards should be set, to apply immediately to the EU institutions;

6. Stresses the importance of involving the relevant sectors in the formulation of policy regarding network security, network integrity and information security in the IP environment;

7. Notes the increasing number of public and private initiatives being taken at international level with a view to ensuring network security, such as the White House Office of Cyberspace Security in the United States, the security information sharing network set up by the G8 and the Europol and Interpol networks;

8. Agrees with the European Council, the Council and the Commission as to the need for a European approach that will enable the internal market in communication services to benefit from common solutions and to operate effectively on the international stage;

9. Points out that network service providers already have an obligation to implement measures aimed at ensuring an appropriate level of data privacy on the basis of Article 17 of the general directive on data protection (95/46/EC), as confirmed in the subsequent provisions on network security and integrity[2];

10. Stresses the need to formulate as soon as possible common definitions regarding network security, network integrity and information security;

11. Calls on the Commission to draw up an action plan to promote the use of electronic signatures, for instance by setting European standards to apply immediately to the EU institutions;

[2] Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector; Directive 97/33/EC on interconnection; Directive 98/10/EC on voice telephony; Directive 1999/93/EC on electronic signatures; and Directive 2000/31/EC on electronic commerce.

As regards institutional considerations

12. Calls on the Commission to supply the European Parliament and the Council with information on problems encountered in implementing the existing directives on data protection, with particular reference to the articles dealing with the issue of network security;

13. Considers that no time must be lost in formulating a European strategy that, while remaining neutral with regard to the type of technology used:

(a) lays down new standards or updates existing standards relating to telecommunications network security and ensures their interoperability,

(b) fosters the development of encryption and certification systems on a European scale and tightens up data protection measures,

(c) ensures that action is taken to prevent and combat crime with due regard for the law,

(d) raises awareness among citizens, users and public and private operators by means of national and European information campaigns aimed at disseminating best practice in this area,

(e) steps up scientific research in the weakest areas, such as the assessment of the security of information technologies, their integration into the overall system, end-user protection and technologies designed to enhance the protection of privacy to include systems like Anti-Echelon/Magic Lantern/Carnivore systems;

14. Agrees with the Commission as to the need to set up at the earliest opportunity a network security task force with the following aims:

- to identify the national authorities responsible for network management;
- to identify the national authorities responsible for coordinating and the chain of command for EU critical and eInfrastructure crisis management;
- to coordinate the activities of those authorities and the pooling of best practice;
- to create a centre of excellence responsible for prevention and information exchange;
- to gather and analyse data on network security issues;
- to analyse current and future security risks;
- to organise discussion forums at European level for those with an interest in security (public authorities, consumers, university researchers, businesses);

15. Calls on the Commission to ensure that this task force takes account in its work of the statements already made in the Cybercrime Forum, and involves the Forum in its future work;

16. Calls on the Commission to formulate clear objectives, after careful consultation with the Member States and the private sector, regarding the objectives, tasks and responsibilities of the planned Task Force, and to ensure that it is supplied with sufficient human and financial resources;

17. Calls on the Commission to give priority to examining the security needs and implementing eInfrastructure early warning system research for networks used for the provision of:
(a) critical infrastructures, essential public services and public health services,
(b) early warning systems and their interoperability,
(c) to foster the development of e-government and e-business;

18. Considers that the first legislative action taken by the Union in this area should be based on its competences in relation to trans-European networks (Title XV of the ECT) and, as regards matters requiring harmonisation, in relation to the internal market (Article 95 of the ECT); considers furthermore that the act laying down the objectives to be pursued at European level should also provide for the setting up of the task force;

19. Calls on the Commission to submit at the earliest opportunity an assessment of the financial impact of Union action in this area, providing comparative data on similar initiatives taken by Member States or third countries (such as the USA);

20. Agrees with the European Council, the Council and the Commission as to the need for a European approach for new legislation or updates to existing legislation relating to investigatory powers, prosecution and penalties for criminal or terrorist activities targeted against critical infrastructures;

21. Calls on the Commission and Council to carry out their deliberations as far as possible within the framework of Eurojust so as to develop a uniform legal basis for the investigation and prosecution of computer criminals;

22. Instructs its President to forward this resolution to the Council and Commission, the governments and parliaments of the Member States, and the Council of Europe.

EXPLANATORY STATEMENT

Introduction

The communication on network and information security, which was published one year ago, sets out a global strategy for electronic network security, as called for by the Stockholm European Council of 23 and 24 March 2001. The communication follows on from the Commission's earlier communication of 8 October 1997, entitled 'Ensuring security and trust in electronic communication' (COM(97) 503).

The approach put forward builds on the framework communication of 22 January 2001 on cybercrime and was taken over and fleshed out by the Telecom Ministers meeting within the Council on 6 December 2001, who adopted a detailed resolution on the matter. It was taken further by the Commission proposal of 19 April 2001 for a framework decision on attacks against information systems.

At its meeting in Barcelona in March 2002 the European Council called on the Commission to draw up a new *e*Europe 2005 action plan whose scope should include network and information security on the basis of a cross-pillar approach. The Commission submitted the action plan to the European Council at its meeting in Seville on 21 and 22 June 2002, where it was adopted

Current state of Community legislation and future prospects

The Community legislative authorities have already taken action in three essential areas relating to network security, namely:

(a) data protection: in particular, **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 (Article 17) and **Directive 97/66/EC** of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (Articles 4 and 5), which will be replaced by the directive adopted by the Council on 25 June 2002 (Cappato report - A5-0130/2002);

(b) telecommunications policies: improving network security is also one of the main concerns of **Directive 99/93/EC** of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and **Directive 2000/31/EC** on electronic commerce. Another aspect of network security is ensuring protection against natural disasters or catastrophic network breakdown (Article 10 of **Directive 97/33/EC** on interconnection and Article 13 of **Directive 98/10/EC** on voice telephony);

(c) combating computer crime: combating cybercrime is one specific aspect of network security. The reference texts in this area are the **Commission communication** on computer-related crime (COM(2000) 890, the **Council recommendation** of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime and the **proposal for a Council framework decision** on attacks against information systems (COM(2002) 173).

The communication attempts to bring these three aspects together into an integrated strategy providing for broad-based action ranging from:

- measures to raise awareness among members of the public and help them learn how to protect themselves

to specific measures such as:

- the setting up of a European warning and information system;
- support for research into security matters;
- standardisation and certification;
- free movement of encryption products;
- security in government use;
- and international cooperation.

Justification for Community action

In the United States the private sector has taken a proactive approach, adopting self-regulatory instruments such as codes of conduct and security programmes. It is in the sector's interest to promote user confidence in networks and to minimise legislative interference.

However, a voluntary approach is not always enough to ensure security, and the main aim of the schemes introduced by private operators is to meet market requirements rather than to address the need to uphold citizens' fundamental rights. Furthermore, private operators such as software vendors are not liable for damage caused by their attitude to security. As the Commission points out in its communication, *'users and providers with low levels of security do not have to pay third party liability'*. This is why the European Union has adopted a legislative approach. The aim is to develop a 'security culture' and foster the exchange of secure information, using instruments that are already on the market but are not sufficiently well-known or are not compatible with one another.

Community action is also justified by the fact that communication and information services are cross-border in nature, as are security threats. Strategic action needs to be taken at European level to foster the development of electronic commerce and establish a genuine internal market in telecommunications and information services which can benefit from common solutions and operate effectively on the world stage. For example, the creation of the European Internet domain name .EU was not merely a means of firmly establishing the European presence in cyberspace; what is more important, it also provides an opportunity to create the sort of trusted environment in cyberspace that the EU has established through the internal market.

Action proposed by the Commission

The European Parliament supports the Commission in its intention to set up an IT security task force, which should be operational by mid-2003. Nonetheless, it calls on the Commission to consider that legislative action in this area should take as its legal basis Title XV of the EC Treaty on trans-European networks and Article 95 ECT for matters regarding the approximation of laws having a bearing on the internal market.

This would ensure that the European Parliament was fully involved in the taking of decisions in an area of such importance to the citizens that it represents.

Glossary:

Server: a remote programme that supplies users with information. Its sole role is to maintain, find and send data to a user in response to that user's request. When a user requires a given document located at a given point on the network, he/she sends the server a request via the Internet. Once the server has received the request, it searches for the relevant data and sends it to the user's computer.
Gateway: connects a set of network computers (for example on a company network) to the Internet, using any type of connection.
Router: a device or program in the computer that determines the nearest point on the network to which the user can be connected to obtain information. The router is connected to at least two networks and decides to which of them the information is to be sent, basing itself on an assessment of the current status of the various networks to which it is connected. Each gateway has a router.

29 May 2002

OPINION OF THE COMMITTEE ON INDUSTRY, EXTERNAL TRADE, RESEARCH AND ENERGY

for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs

on the communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions entitled 'Network and information security: proposal for a European policy approach'
(COM(2001) 298 – C5-0657/2001 – 2001/2280 (COS))

Draftsman: W.G. van Velzen

PROCEDURE

The Committee on Industry, External Trade, Research and Energy appointed W.G. van Velzen draftsman at its meeting of 22 November 2001.

The committee considered the draft opinion at its meetings of 16 April and 22 May 2002.

At the latter meeting it adopted the following conclusions unanimously.

The following were present for the vote: Carlos Westendorp y Cabeza (chairman), Peter Michael Mombaur and Yves Piétrasanta (vice-chairmen), W.G. van Velzen (draftsman), Nuala Ahern, Sir Robert Atkins, María del Pilar Ayuso González (for Jaime Valdivielso de Cué), Guido Bodrato, David Robert Bowe (for Norbert Glante), Marco Cappato, Massimo Carraro, Gérard Caudron, Giles Bryan Chichester, Willy C.E.H. De Clercq, Concepció Ferrer, Francesco Fiori (for Umberto Scapagnini), Christos Folias (for Christian Foldberg Rovsing), Michel Hansenne, Hans Karlsson, Bashir Khanbhai, Bernd Lange (for Rolf Linkohr), Werner Langen, Caroline Lucas, Marjo Matikainen-Kallström, Eryl Margaret McNally, William Francis Newton Dunn (for Nicholas Clegg), Angelika Niebler, Reino Paasilinna, Paolo Pastorelli, Elly Plooij-van Gorsel, Samuli Pohjamo (for Colette Flesch), Godelieve Quisthoudt-Rowohl, Paul Rübig, Konrad K. Schwaiger, Alejo Vidal-Quadras Roca, Dominique Vlasto, Anders Wijkman (for John Purvis), Myrsini Zorba and Olga Zrihen Zaari.

SHORT JUSTIFICATION

Security plays a role in every aspect of daily life. Individuals and companies are expected first and foremost to be aware of and accept their responsibilities regarding their own security and that of their (immediate) surroundings. By extension this also applies to electronic communications networks. The internet routinely suffers massive disruption. Rapidly propagated e-mail viruses soon awoke users to the risks involved and to the vulnerability of their computer systems. At a time when electronic communications networks are converging rapidly, it is important to further heighten awareness of this problem and the possible risks arising.

In addition to the known threat posed by computer viruses, electronic communications network security is beset by many other hazards. Not only e-mail viruses but also the possible interception of communications, use of false identities or unauthorised network access are real risks of which users should be aware, in addition to the risk of non-malicious human error or natural disasters.

Furthermore the availability of electronic communications networks is of increasing importance for other infrastructures, such as water and energy supply. Increasing network convergence therefore increases the dependence and vulnerability of our (information) society.

On the principle that prevention is better than cure, it is essential to be aware of the situation and the first task of the government should be to ensure that individuals and companies are able to protect themselves against certain security risks. The authorities have an important task to fulfil in providing information, part of which should be the formulation of sound, commonly accepted definitions regarding network security, network integrity and the security of information.

Computer warning systems can be used to contain as rapidly as possible an attack already being launched or any other threat. Existing CERT[1] initiatives (taken by governments and large companies) are an example of such a system. They should, however, be made available to all users, including individuals and small(er) companies. This is also a major government task. Existing CERTs should be extended and made to function properly at Member State level before any moves are made to set up a European CERT.

Ideas and actions to improve security are only effective if all can benefit. In other words, the effectiveness of measures to increase security is undermined if different non-interoperable solutions are chosen. It is therefore crucial that they be based on open international standards. While there has been no lack of effort in the field of standardisation, numerous competing standards and specifications have resulted in market fragmentation and lack of interoperability. Solutions on the basis of open source software can help make it possible to correct mistakes more quickly and ensure greater transparency, which is conducive to greater security. Solutions to improve network security should therefore be sought in cooperation with all relevant sectors. As well as taking suitable action it is necessary to monitor continuously at international level the degree of vulnerability and the effectiveness of certain

[1] Computer Emergency Response Team.

measures. Benchmarking can be a useful instrument for keeping track. Given the global nature of electronic communications networks and hence the security risks, it is necessary to enter into dialogue with other countries and their institutions so as to be immediately informed of any risks arising or compare notes concerning measures to be taken and policy implementation.

In view of the frequently criminal nature of threats to network security (except of course natural disasters or human error), network safety measures should, as far as possible, form part of the Eurojust initiatives in order to provide a uniform legal framework for cybercrime detection and prosecution.

CONCLUSIONS

The Committee on Industry, External Trade, Research and Energy calls on the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, as the committee responsible, to incorporate the following points in its motion for a resolution:

having regard to the rapid convergence of electronic communications networks which are increasingly becoming a key factor in economic and social terms,

A. whereas, as a result of this convergence, it is necessary to create an adequate policy and legal framework in the European Union to guarantee the protection of network and information security, which is an essential precondition for existence of the Information Society,

B. whereas measures to improve security can only be effective if all those concerned, including individual citizens, are aware of the security risks and their own responsibility regarding precautions to be taken,

C. whereas solutions to increase safety are only effective if they are applied by all the market players concerned, preferably on the basis of open international standards,

D. whereas the Computer Emergency Response Teams (CERTs) operate in different ways in different Member States, thereby unnecessarily complicating efforts to achieve cooperation,

1. Stresses the need to formulate as soon as possible common definitions regarding network security, network integrity and information security;

2. Welcomes the Commission’s plan to set up a Cyber Security Task Force, and urges the Council to put this plan into practice as soon as possible and to establish the Task Force by the end of 2002;

3. Calls on the Commission to formulate clear objectives, after careful consultation with the Member States and the private sector, regarding the objectives, tasks and responsibilities of the planned Task Force, and to ensure that it is supplied with sufficient human and financial resources;

4. Instructs the Commission to accord the Task Force at all events the role of an independent European centre of competence for network and information security, so as to enable it not only to operate, inter alia, as a source of information for Member States on the formulation of national policy and as an independent advisor for Member States and the private sector, but also to carry out investigations independently in the field of network and information security;

5. Emphasises the need to ensure as soon as possible that all citizens, businesses and administrations have access to the public electronic services of all EU administrations via a secure and personalised authenticated access system; considers that in order to

ensure this, electronic signatures should be used and European standards should be set, to apply immediately to the EU institutions;

6. Calls on the Commission to initiate greater awareness on the part of individuals, companies and the public sector regarding electronic communications networks security risks and to play a leading role in coordinating the substance of information campaigns in Member States concerning the safety aspects and risks arising from electronic communications networks and instructs the Commission to allocate this task in the first instance to the Cyber Security Task Force shortly to be set up;

7. Calls on the Commission to draw up an action plan to promote the use of electronic signatures, for instance by setting European standards to apply immediately to the EU institutions;

8. Stresses the importance of involving the relevant sectors in the formulation of policy regarding network security, network integrity and information security in the IP environment;

9. Welcomes the Commission's plans to cooperate with the Member States in investigating the best way of organising the collection and analysis of information and the planning of preventive measures against present and future security risks;

10. Calls on the Commission and Council to carry out their deliberations as far as possible within the framework of Eurojust so as to develop a uniform legal basis for the investigation and prosecution of computer criminals.