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

Network and Information Security: Proposal for a European Policy Approach

Table of contents

1. Introduction

Concerns about security of electronic networks and information systems have been growing along with the rapid increase in the number of network users and the value of their transactions. Security has now reached a critical point where it represents a prerequisite for the growth of electronic businesses and the functioning of the whole economy. Several factors have combined to push information and communication security to the top of the policy agenda in the EU:

- Governments have realised the extent to which their economies and their citizens are dependent on the effective working of communication networks and several have begun to review their security arrangements.

- The Internet has created a global connectivity linking together millions of networks, large and small, and hundreds of millions of individual PCs, and increasingly other devices including mobile phones. This has significantly reduced the costs of accessing valuable economic information for remote attackers.

- There have been some widely reported viruses released onto the Internet causing extensive damage by destroying information and denying access to the network. Such security problems are not confined to individual countries but spread quickly across Member States.

- The Lisbon and Feira European Councils recognised the Internet as a key driver in the productivity of EU economies when launching the *e*Europe 2002 Action Plan.

Against this background the Stockholm European Council on 23-24 March 2001 concluded *"the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action. This should be presented in time for the Göteborg European Council."* This Communication is the European Commission's response to this request.

A changing environment

Whilst security has become a key challenge for policy makers, finding an adequate policy response is becoming an increasingly complex task. Only a few years ago, network security was predominantly an issue for state monopolies offering specialised services based on public networks, in particular the telephone network. Security of computer systems was limited to large organisations and focused on access controls. Establishing a security policy was a relatively straightforward task. This situation has now changed considerably because of a variety of developments in the wider market context, amongst them liberalisation, convergence and globalisation:

Networks are now mainly privately owned and managed. Communication services are offered on a competitive basis with security as part of the market offer. However many customers remain ignorant of the extent of the security risks they run when connecting to a network and are therefore making their decisions in a situation of incomplete information.

Networks and information systems are converging. They are becoming increasingly interconnected, offering the same kind of seamless and personalised services and to some extent

sharing the same infrastructure. End terminals (PCs, mobile phones, etc.) have become an active element in the network architecture and can be connected to different networks.

Networks are international. A significant part of today's communication is cross border or transits through third countries (sometimes without the end-user being aware of it), so any solution to a security risk needs to take account of this. Most networks are built using commercial products from international vendors. Security products must be compatible with international standards.

Policy relevance

These developments constrain the ability of governments to influence the level of security of the electronic communications of their citizens and businesses. This does not mean however that the public sector no longer has a role for a number of reasons:

Firstly, **there are several legal measures in place at Community level with specific implications for network and information security**. In particular the European telecommunications and data protection framework contains provisions for operators and service providers to ensure a level of security appropriate to the involved risks.

Secondly, there are growing concerns about **national security** as information systems and communication networks have become a critical factor for other infrastructures (e.g. water and electricity supply) and other markets (e.g. the global finance market).

Finally, there are reasons why action by governments is required in response to **imperfections in the market**. Market prices do not always accurately reflect the costs and benefits of investment in improved network security and neither providers nor users always bear all the consequences of their behaviour. Control over the network is dispersed and weaknesses in one system can be exploited to attack another. The complexity of networks makes it difficult for users to assess potential dangers.

It is therefore the objective of this Communication to establish where additional or enhanced public action at European or national level is required.

Chapter 2 defines network and information security, describes the main security threats and assesses the current solutions. It aims at providing a level of understanding of network and information security necessary to illuminate the proposed policy solutions. It is not the intention to give an exhaustive technical overview of security issues.

Chapter 3 proposes a European policy approach aimed at improving network and information security. It is based on an analysis of the need to supplement market solutions with policy actions. It lists a series of concrete policy measures, as was requested by the Stockholm European Council. The proposed policy should be seen as an integral element of the existing framework for electronic communication services and data protection and – more recently – cyber-crime policy.

2. Analysis of network and information security issues

2.1. What is network and information security?

Networks are systems on which data are stored, processed and through which they circulate. They are composed of transmission components (cables, wireless links, satellites, routers, gateways, switches etc) and support services (domain name system including the root servers, caller identification service, authentication services, etc). Attached to networks is an increasingly wide range of applications (e-mail delivery systems, browsers, etc.) and terminal equipment (telephone set, host computers, PCs, mobile phones, personal organisers, domestic appliances, industrial machines, etc.).

The generic security requirements of networks and information systems can be considered to consist of the following interrelated characteristics:

i) **Availability** – means that data is accessible and services are operational, despite possible disruptive events such as power supply cuts, natural disasters, accidents or attacks. This is particularly vital in contexts where communication network failures can cause breakdowns in other critical networks such as air transport or power supply.

ii) **Authentication** – is the confirmation of an asserted identity of entities or users . Proper authentication methods are needed for many applications and services such as concluding a contract online, controlling access to certain data and services (e.g. for teleworkers) and authentication of websites (e.g. for Internet banks). Authentication must also include the possibility for **anonymity,** as many services do not need the identity of the user, but only reliable confirmation of certain criteria (so-called anonymous credentials) such as the ability to pay.

iii) **Integrity** – is the confirmation that data which has been sent, received, or stored are complete and unchanged. This is particularly important in relation to authentication for the conclusion of contracts or where data accuracy is critical (medical data, industrial design, etc.).

iv) **Confidentiality** – is the protection of communications or stored data against interception and reading by unauthorised persons. It is particularly needed for the transmission of sensitive data and is one of the requirements to address privacy concerns of users of communication networks.

All events which threaten security need to be covered, not just those with malicious intent. From a user's point of view, threats such as environmental incidents or human errors which disrupt the network are potentially as costly as malicious attacks. **Network and information security can thus be understood 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.**

2.2. Overview of security threats

Companies relying on the network for sales or to organise delivery of supplies can be paralysed by a denial of service attack. Personal and financial information can be intercepted and abused. National security can be threatened. These examples give an indication of the threats of inadequate security. A distinction is made between intentional attacks (sections 2.2.1 to 2.2.5) and unintentional events (section 2.2.6). The objective of these sections is to specify the type of

security risks in order to lay the basis for the establishment of a policy framework to improve security in section 3.

2.2.1. Interception of communications

Electronic communication can be intercepted and data copied or modified. Interception can be undertaken in a number of ways. These include the physical accessing of network lines, e.g. wire tapping, and monitoring radio transmissions. The most critical points for the interception of communication traffic are the network management and concentration points, such as routers, gateways, switches and network operation servers.

Malicious or unlawful interception of communications must be distinguished from lawful interception activities. Interception of communications for reasons of public security is authorised in specific cases for limited purposes in all EU Member States. A legal framework is in place to allow law enforcement agencies to obtain judicial orders, or in the case of two Member States, a warrant personally authorised by a senior Minister, to intercept communications.

Potential damage - Unlawful interception can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted, such as passwords or credit card details, for commercial gain or sabotage. This is perceived to be one of the biggest inhibitors to the take-up of e-commerce in Europe.

Potential solutions - Defence against interception can be made by **operators** securing the network as they are required to do inter alia under Directive 97/66 EC [1] and by **users** encrypting data transmitted over the network.

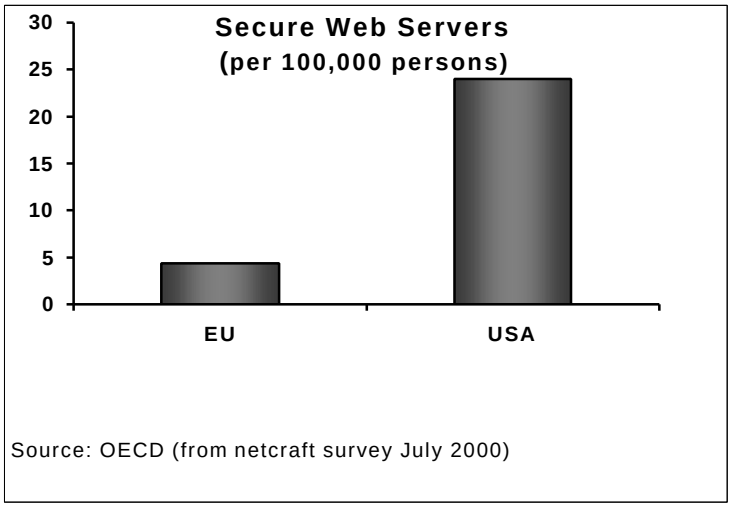
For **operators**, protection of the network against potential interception is a complex and expensive task. Traditionally, telecom operators have secured the network through physical access controls to installations and guidelines for employed staff. Traffic was only occasionally encrypted. Where wireless solutions are deployed, there is an onus on ensuring that the radio transmissions are adequately encrypted. Mobile communication operators encrypt traffic between the mobile phone and the base station. The strength of encryption in most EU countries is lower than is technically feasible because of the requirements to facilitate legal interception. For the same reason the encryption can be switched on and off from the base stations without the user being aware of it.

Users can make their own decision to encrypt data or voice signals independently of network security provisions. Properly encrypted data is incomprehensible to all but the authorised recipient, even if intercepted. Encryption software and hardware is widely available for practically all types of communications [2]. Special products can encrypt a telephone conversation or a fax transmission. E-mails can be encrypted using special software or software integrated into a word processor or e-mail client. The problem for the users is that if they encrypt e-mail or voice communications the recipient must be able to understand it. Equipment or software must be interoperable. They also need to know the decryption key, which means that there should be a mechanism to receive the key including proper authentication of the key. The cost of encryption in both money and effort is significant and users often lack information about security risks and benefits and this makes it difficult for them to take the best decisions.

---

[1] Directive on data protection in telecommunications (OJ L 24 of 30.1.1998).

[2] See Commission Communication on "Ensuring security and trust in electronic communication", 8 October 1997, COM (1997) 503 final.



Source: OECD (from netcraft survey July 2000)

A commonly used secure system on the Internet is the "Secure Socket Layer" (SSL). SSL encrypts the communication between a web server and a user's web browser. An inhibiting factor in the take-up of this technology, especially the strongest version (128 bit), has been the past restrictive export controls of the US The US export control regime has been recently revised following the adoption of a more liberal Community regime for the control of exports of dual use items and technologies [3] . Statistics indicate that the number of secure web servers in Europe lags far behind the US (see graph).

Operators, users and producers face the problem of competing and non-interoperable standards. For example in the secure e-mail field, two standards [4] are competing to become dominant. Europe's influence here has been limited. The result is a profusion of non-European products that implement these standards and where access for European users depends on the export control policy of the United States. While there is concern in relation to the level of security offered by many of these products (c.f. Echelon [5]), some EU governments are considering the use of open source software to increase the level of confidence in encryption products. However, this is in the pilot stage [6], not yet co-ordinated and market forces may simply be stronger than isolated government efforts. This issue can be addressed by conducting a comprehensive evaluation of both the commercial and open-source products.

2.2.2. Unauthorised access into computers and computer networks

Unauthorised access to a computer or network of computers is usually done with malicious intent to copy, modify or destroy data. Technically this is called intrusion and can be done in many ways including exploiting inside information, dictionary attacks, brute force attacks (exploiting people's tendency to use predictable passwords), social engineering (exploiting people's tendency to disclose information to seemingly trustworthy people) and password interception. It is often performed from within the organisations (inside attacks).

Potential damage - Some unauthorised intrusion is motivated by intellectual challenge rather than monetary gain. However, what began as a nuisance activity (often described as 'hacking') has highlighted the vulnerabilities of information networks and motivated those with criminal or malicious intent to exploit these weaknesses. Protection against unauthorised access to their personal information, including their financial details, bank accounts and health information, is a

[3] Council Regulation (EC) N° 1334/2000 setting up a Community regime for the control of exports of dual use items and technologies (OJ L 159 of 30.06.2000).

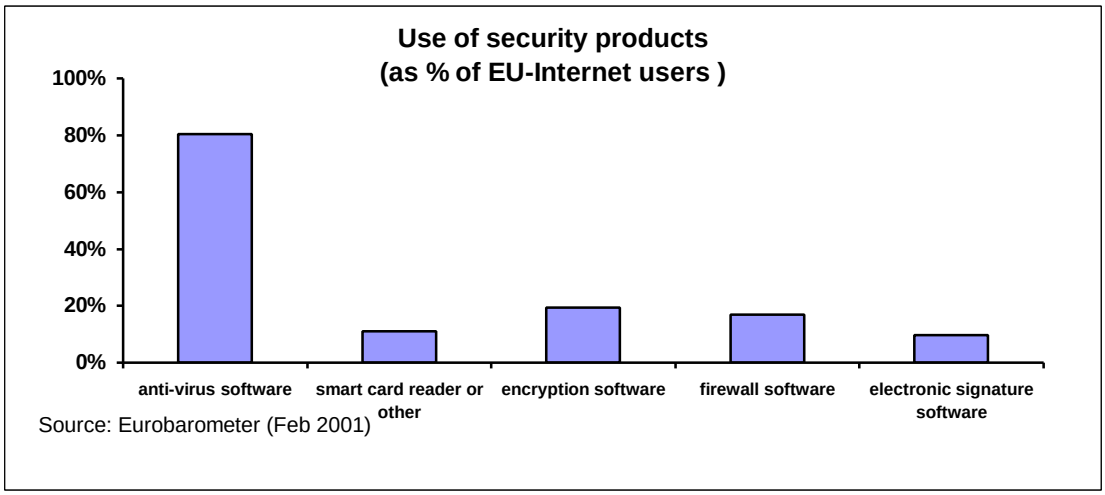
[4] S-MIME (secure multiple Internet mail extensions) and OpenPGP (Pretty Good Privacy) are both IETF (Internet Engineering Task Force) standards.

[5] The ECHELON system is allegedly used to intercept ordinary e-mail, fax, telex and telephone communications carried over the world's telecommunications networks. See also the activities of the European Parliament Temporary Committee on Echelon at http://www.europarl.eu.int/committees/echelon_home.htm

[6] The German government is funding a project based on the OpenPGP standard and is called GNUPG (http://www.gnupg.org).

right of individuals. For the public sector and industry, the threats range from economic espionage to the potential modification of internal or public data, including the corruption of web sites.

Potential solutions - The most common methods of protecting against unauthorised access are password controls and installation of firewalls. However, these give only limited protection and need to be complemented by other security controls which could include attack recognition, intrusion detection and application level controls (including those involving smart cards). The effectiveness of the controls is dependent on how their functionality matches the risks related to a specific environment. A balance must be achieved between network protection and the advantages of free access. Due to rapid changes and consequent new threats to networks there is a need for ongoing independent review of network security controls. Until users and providers



are fully aware of the potential vulnerability of their network, potential solutions will remain unexplored. An overview of the current use of security products in the European Union is provided in the above graph (statistics are based on a survey carried out in February 2001 in the context of the *e*Europe 2002 benchmarking exercise).

2.2.3. Network disruption

Networks are now largely digitised and controlled by computers. In the past a common reason for network disruption was a failure in the computer system that controls the network and attacks on networks were mainly directed towards these computers. Nowadays, the most disrupting attacks tend to exploit the weaknesses and vulnerabilities of network components (operating systems, routers, switches, name servers, etc.).

Whilst disruptive attacks on the telephone system have not been a major concern in the past, attacks on the Internet are quite common. This is due to the fact that telephone control signals are separated from traffic and can be protected whereas the Internet allows users to reach the key management computers. However, the telephone network may become more vulnerable in future as it will integrate key elements of the Internet and its control plan will be opened to others.

Attacks may take various forms:

- **Name server attacks**: The Internet depends on the operation of the Domain Name System (DNS) through which user-friendly names (e.g. europa.eu.int) are translated into abstract network addresses (e.g. IP n° 147.67.36.16) and vice versa. If part of the DNS fails, some web sites cannot be located and email delivery systems may stop working. Corruption at the level of DNS root servers or other top level name servers could lead to widespread

disruption. Earlier this year some vulnerabilities were discovered in the software on which most name servers operate [7].

- **Routing attacks**: Routing in the Internet is highly decentralised. Each router periodically informs neighbouring routers about which networks it knows and how to reach them. The weakness is that this information cannot be verified because, by design, each router's knowledge of network topology is minimal. In consequence, any router can represent itself as a best path to any destination as a way of intercepting, blocking or modifying traffic to that destination.

- **Flooding and denial of service attacks**: These forms of attack disrupt the network by overloading it with artificial messages which deny or reduce legitimate access. It is similar to fax machines being blocked by long and repeated messages. Flooding attacks attempt to overload web servers or the handling capacity of Internet Service Providers (ISPs) with automatically generated messages.

Potential damage - Interruptions have been damaging for certain high-profile websites. Some studies have calculated several hundreds of millions of Euro of damage from a recent attack, in addition to the intangible damage to reputation. Increasingly companies rely on the availability of their websites for their business and those companies that depend on it for 'just in time' supply are particularly vulnerable.

Potential solutions - Attacks on DNS servers are, in principle, easily dealt with by extending the DNS protocols, for example using secure DNS extensions based on public key cryptography. However, this involves installing new software on client machines and has not been widely deployed. Also, the administrative process required to enhance the trust between DNS domains needs to become more effective.

Attacks on the routing system are much harder to defend. The Internet was designed to maximise flexibility in routing as this reduces the probability of service being lost if one part of the network infrastructure breaks down. No effective means exist to secure routing protocols, especially on backbone routers.

The volume of data transmitted does not allow for detailed filtering as such verification would bring the networks to a halt. For that reason only basic filtering and access control functions are performed by the networks, whereas more specific security functions (e.g. authentication, integrity, encryption) are placed at the boundaries of the networks i.e. on the terminals and network servers that act as end points.

2.2.4. Execution of malicious software that modifies or destroys data

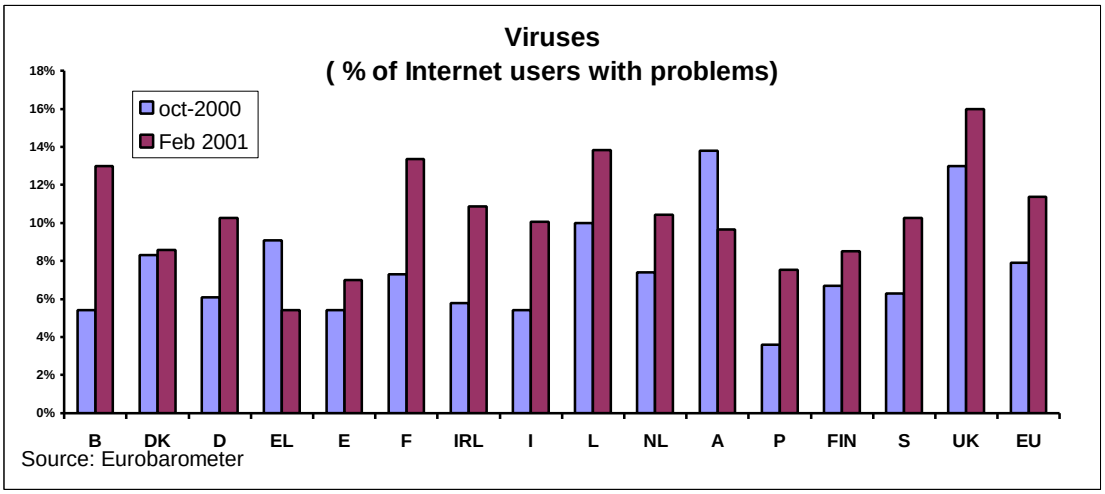
Computers run with software. Software can unfortunately also be used to disable a computer, to delete or modify data. As the above descriptions show, if such a computer is part of the network management its malfunctioning can have far-reaching effects. A virus is one form of malicious software. It is a program that reproduces its own code by attaching itself to other programs in such a way that the virus code is executed when the infected computer program is executed.

There are various other types of malicious software: some damage only the computer on which they are copied and others spread themselves to other networked computers. For instance there are programmes (dramatically called 'logic bombs') that lie dormant until triggered by some event

[7] Source CERT/CC at http://www.cert.org/advisories/CA-2001-02.html

such as a specific date, - Friday the 13th - is often used**.** Other programmes appear to be benign but when opened release a malicious attack (therefore called 'Trojan Horses'). Other programmes (called 'worms') do not infect other programs as a virus will, but instead make copies of themselves, which consequently create even more copies to eventually swamp the system.

Potential damage - Viruses can be very destructive as illustrated by the high costs associated with some recent attacks (e.g. 'I Love you', 'Melissa' and 'Kournikova'). The following chart gives an overview of the increase of viruses EU Internet users have encountered between October 2000 and February 2001 (by Member State). On average about 11 % of European Internet users have caught a virus on their home PC.



Potential solutions - The main defence is anti-virus software, which is available in various forms. For instance virus scanners and disinfectors identify and delete known viruses. Their main shortcoming is that they will not easily pick up new viruses even when updated regularly. Another example of anti-virus defence is an integrity checker. In order for a virus to infect a computer, it must change something on that system. The integrity check could identify these changes even when caused by unknown viruses.

Despite relatively well-developed defence products, problems with malicious software have increased. There are two main reasons. Firstly, the openness of the Internet allows attackers to learn from each other and develop methods to circumvent protection mechanisms. Secondly the Internet is growing and reaching more users, many of which are unaware of the need to take precautionary measures. Security will depend on the extent to which defence software is used.

2.2.5. Malicious misrepresentation

When establishing a network connection or receiving data the user makes assumptions on the identity of their interlocutor based on the context of the communication. The network offers certain indicators but the greatest risk of attack comes from people who know the context i.e. insiders. When users dial a number or type an Internet address into the computer they should reach the expected destination. This is sufficient for many applications, but not for key business, medical, financial or official interactions which require a higher level of authentication, integrity and confidentiality.

Potential damage - Misrepresentation of people or entities can cause damage in various ways. Customers may download malicious software from a website masquerading as a trusted source. They may release confidential information to the wrong person. There is the possibility of misrepresentation leading to repudiation of contracts etc. Perhaps the greatest damage is the fact that lack of authentication is holding back potential business. Many studies have highlighted

security worries as a principal reason for not doing business over the Internet. If people could be certain that their interlocutor is who they say they are, the level of confidence in Internet transactions would increase.

Potential solutions - Attempts to introduce authentication into the networks linked to the introduction of SSL is already useful in ensuring a certain level of confidentiality. Virtual Private Networks (VPN) use SSL and IPsec to enable communications to run over insecure Internet and open channels while maintaining a given security level. However, these solutions are limited in their usefulness as they are based on electronic certificates and there is no guarantee that these certificates are not forged. A third party, often referred to as 'Certification Authority' or in the e-signatures Directive [8] a 'Certification Service Provider', can offer such assurance. The problem for widespread uptake of this solution is similar to that faced in encryption - the need for interoperability and key management. In a VPN this is not a problem as proprietary solutions can be developed but for public networks it is a major barrier.

The e-signature Directive enhances the legal basis to assure easier electronic authentication in the EU. It provides a framework where the market is free to develop, but which also provides incentives to develop more secure signatures for legal recognition. The transposition of the Directive into national law is currently in process.

2.2.6. Environmental and unintentional events

Many security incidents are due to unforeseen and unintentional events caused by

- natural disasters (e.g. **s**torms, floods, fires, earthquakes)
- third parties without any contractual relation with the operator or the user (e.g. interruption of service because of construction works)
- third parties with a contractual relation with the operator or the user (e.g. hardware or software failures in delivered components or programs)
- human error or poor management of the operator (including the service provider) or the user (e.g. problems in network management, incorrect installation of software).

Potential damage: Natural disasters cause disruption in the availability of networks. Unfortunately it is during such events that functioning communication lines are most needed. Hardware failures and poor software design can create vulnerabilities which cause immediate disruption or are exploited by attackers. Poor management of network capacity can lead to congestion that slows down or disrupts the communication channels.

In this context, a crucial question is the distribution of liabilities amongst parties. In most cases the users will have no responsibility but may find themselves with little or no possibilities for liability claims.

Potential solution: The risks of environmental incidents are known to telecommunication network operators and they have built redundancies and infrastructure protection into their networks. Increasing competition could have an ambivalent impact on the behaviour of operators. On the one hand price considerations may drive operators to reduce these redundancies and on the other hand the existence of more operators in the market as a result of liberalisation enable users to switch to another operator in case of unavailability (much like an air

[8] Directive 1999/93/EC of 13 December 1999 establishing a common framework for electronic signatures (OJ L 13 of 19.1.2000, p. 12).

passenger is switched to another air line when a flight is cancelled). However relevant Community law requires that Member States take all necessary steps to ensure the availability of public networks in the event of catastrophic network breakdown or natural disasters (c.f. Interconnection Directive 97/33/EC [9] and Voice telephony Directive 98/10/EC [10]). Overall, in this area, too little is known about the level of security as a result of the increasing number of interconnected networks.

Competition amongst hardware and software vendors should exert pressure to improve the security of their products. However competition is not strong enough to drive security investments and security is not always the key element in the buying decision. Security flaws are often discovered too late, when the damage has already been done. The preservation of fair competition behaviour in the markets for information technology will create better security conditions.

The risk of human error and operating mistakes can be reduced by improved training and awareness raising. The establishment of an appropriate security policy at company level would help to reduce these risks.

2.3. New challenges

Network and information security is likely to become a key factor in the development of the information society as networking plays a larger role in economic and social life. There are two main issues to consider: the increasing potential damage and new technological developments.

i) Networks and information systems carry more and more **sensitive data and economic valuable information** which will increase the incentive for attacks. These attacks can be low-level and inconsequential on a national scale – e.g. in the case of the defacement of a personal web site or the reformatting of a hard disk by a virus. However, the disruption can also be on a much more critical scale, up to the level of interference with highly sensitive communications, significant power cuts, or major loss of business through denial of service attacks or confidentiality breaches.

   The exact extent of actual and potential damage due to breaches in network security is difficult to assess. There is no systematic reporting system and many companies prefer not to admit encountered attacks for fear of negative publicity. Thus the evidence that exists is mainly anecdotal. Costs involved consist not just of direct costs (loss of revenue, loss of valuable information, manpower costs to restore the network), but there are many intangible costs associated with attacks - particularly loss of reputation - which are difficult to assess.

ii) **Network and information security is a dynamic issue**. The speed of technology change poses permanent new challenges, problems of yesterday disappear and today's solutions are meaningless. The market offers new applications, services and products on an almost daily basis. However, there are some developments which will clearly pose significant challenges to a private and public security policy:

   - Different digital objects will be transmitted on the networks such as multimedia objects, downloadable software or mobile agents with incorporated security policies. The notion of availability perceived today as the ability to use the networks will evolve in terms of authorised usage e.g. right to use a video game for a certain period, right to create a single copy of a software program, etc.

[9] OJ L 199 of 26.07.1997.
[10] OJ L 101 of 01.04.1998.

- In the future, operators of IP-networks may want to increase security by continually auditing the network traffic in order to only allow authorised traffic. Such measures however must be in accordance with relevant data protection rules.

- Users will switch to having 'always-on' Internet connections, which widen the window of opportunity for attackers and create vulnerabilities for unprotected terminals, and make it easier for attackers to avoid detection.

- Home networks connecting a variety of appliances will be widely introduced, opening up new avenues of attack and increasing user vulnerability (for example alarms could be turned off remotely).

- Large-scale introduction of wireless networks (e.g. wireless local loop, wireless local area networks, third generation mobile) will bring the challenge of effectively encrypting data transmitted over radio signals. It will therefore be increasingly problematic to require by law weak encryption of those signals.

- Networks and information systems will be everywhere, combining fixed and wireless and offering 'ambient intelligence', i.e. self-organisational functions that run automatically and make decisions formerly taken by the user. The challenge will be to avoid unacceptable vulnerabilities and integrate security into the architectures.

3. A European policy approach

3.1. Rationale for public policy

Protecting communication networks is increasingly considered as a priority for policy makers mainly because of data protection, ensuring a functioning economy, national security, and the wish to promote e-commerce. This has led to a substantial body of legal safeguards in EU Directives on data protection and in the EU regulatory framework for telecommunications (as demonstrated in section 3.6). These measures however have to be applied in a rapidly changing environment of new technologies, competitive markets, convergence of networks, and globalisation. These challenges are compounded by the fact that the market will tend to under invest in security for reasons analysed below.

Network and information security is a commodity bought and sold on the market and part of the contractual agreements between parties. The market for security products has grown substantially over the past few years. According to some studies the market for Internet security software was worth around $4.4 billion worldwide at the end of 1999 [11] and will grow 23 % per annum to reach $ 8.3 billion in 2004. In Europe, the electronic communication security market is forecast to grow from $465 million in 2000 to $5.3 billion in 2006 [12], with the security market for information technologies growing from $490 million in 1999 to $2.74 billion in 2006 [13].

The implicit assumption usually made is that the price mechanism will balance the costs of providing security with the specific need for security. Certain users will request high security whilst others will be satisfied with a lower level of assurance – although the State may provide for a minimum level of security. Their preferences would be reflected in the price they are willing to pay for security features. However – as shown by the analysis of section 2 – many security risks

[11] IDC : Internet security market forecast and analysis, 2000-2004 Report #W23056 - October 2000
[12] Frost&Sullivan : The European Internet communication security markets, report 3717 - November 2000
[13] Frost&Sullivan : The European Internet system security markets, report 3847 - July 2000

remain unsolved or solutions are slow coming to the market as a result of certain market imperfections:

i) **Social costs and benefits:** Investment in improved network security generates social costs and benefits which are not adequately reflected in market prices. **On the cost side**, market actors are not responsible for all the liabilities related to their security behaviour. Users and providers with low levels of security do not have to pay third party liability. This is like a careless car driver who is not held liable for the costs of the traffic jam that occurred as a result of his accident. Similarly, on the Internet several attacks have been mounted through the ill-protected machines of relatively careless users. **Security benefits are also not fully reflected in market prices**. When operators, suppliers, or service providers improve the security of their products a good deal of the benefits of this investment accrue not only to their customers but to all those directly or indirectly affected by electronic communication - basically the whole economy.

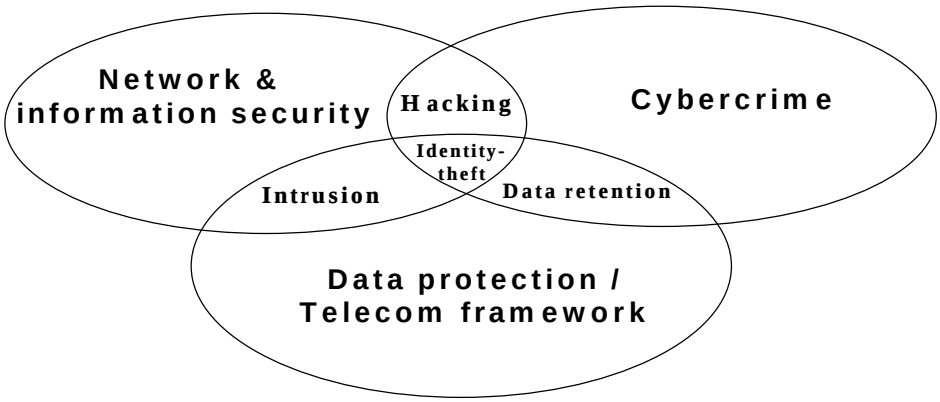
ii) **Asymmetry of information:** Networks are becoming increasingly complex and are reaching a wider market that includes many users with little understanding of the technology or its potential dangers. This means users will not be fully aware of all the security risks and many operators, vendors, or service providers have difficulties assessing the existence and widespread of vulnerabilities. Many new services, applications and software offer attractive features but often these are the source of new vulnerabilities (e.g. the world wide web's success is partly due to the range of multimedia applications that can be easily downloaded but these 'plug-ins' are also an entry point for attacks). Whilst the benefits are visible, the risks are not and there are more incentives for suppliers to offer new features than greater security.

iii) **The public action problem:** Operators are increasingly adopting the Internet standards or somehow linking their networks to the Internet. However, the Internet was not designed with security in mind but on the contrary was developed to ensure access to information and to facilitate its exchange. This has been the basis for its success. The Internet has become a global network of networks of unparalleled richness and diversity. Investment in security often only pays off if enough people do the same. Thus **co-operation** to create security solutions is required. But co-operation only works if a critical mass of players participates which is difficult to achieve as there are 'free-rider' profits to be made. Interoperability between products and services will allow for competition between security solutions. However there are substantial co-ordination costs involved as global solutions might be required and some players are tempted to impose a proprietary solution on the market. As a multitude of products and services still uses proprietary solutions there is no advantage to using secure standards which only give extra security if everyone else offers them.

As a result of these imperfections the telecommunications and data protection framework already provides for legal obligations for operators and service providers to ensure a certain level of security in communication and information systems. The rationale for a European policy on network and information security can be described as follows. Firstly, the legal provisions at EU level need to be applied effectively which requires **a common understanding of the underlying security issues and the specific measures to be taken**. The legal framework will also need to evolve in the future as already can be seen by the proposed new regulatory framework for electronic communications or the forthcoming proposals linked to the cyber-crime discussion. Secondly, certain market imperfections lead to the conclusion that market forces do not drive sufficient investment into security technology or security practice**. Policy measures can reinforce the market process and at the same time improve the functioning of the legal framework.** Finally, communications and information services are offered across borders. Therefore, a European policy approach is

needed **to ensure the Internal Market for such services, to benefit from common solutions, and to be able to act effectively on global level**.

The proposed policy measures with regard to network and information security have to be seen not only in the context of the existing telecommunications and data protection legislation but also in relation to the more recent cyber-crime policies. The Commission has recently published a Communication on cyber-crime [14] which foresees, amongst other initiatives, the setting up of an EU Forum on cyber-crime with the aim of enhancing mutual understanding and co-operation at EU level between all interested parties. A network and information security policy will provide the missing link in this policy framework. The diagram below shows these three policy areas and illustrates with a few examples how they are interrelated:



3.2. Awareness raising

Too many users (private/public) are still not aware of the possible threats they encounter when using communication networks or of the solutions that already exist to tackle them. Security issues are complex and risks are often difficult, even for experts, to assess. Lack of information is one of the market imperfections that security policy should address. There is a risk that some users, alarmed by the many reports of security threats, simply choose to avoid e-commerce altogether. Others who are either uninformed or underestimate the risk may be too careless. Some companies may have an interest in underplaying potential risks, for fear of losing customers.

Paradoxically there is a huge amount of information on network and information security available on the Internet and computer magazines cover this issue quite extensively. The problem for users is to find appropriate information that is understandable, up-to-date and responds to their particular needs. The automobile industry gives a good example of how complex safety specifications can be transformed into a key marketing feature. Finally, the service providers of a publicly available telecommunications service are obliged under EU law to inform their subscribers concerning particular risks of a breach of security of the network and any possible remedies, including the costs involved (c.f. article 4 of Directive 97/66/EC).

The aim of an awareness raising initiative for citizens, administrations and businesses is therefore to provide accessible, independent and reliable information on network and information security.

---

[14] Creating a safer society by improving the security of information infrastructures and combating computer related crime, COM (2000) 890, http://europa.eu.int/ISPO/eif/internetPoliciesSite/Crime/crime1.html

An open discussion on security is needed. Once awareness is assured people are free to make their own choices on the level of protection that they are comfortable with.

Proposed actions:

- Member States should launch a public information and education campaign and ongoing work needs to be upgraded. This should comprise a mass media campaign and action targeted at all stakeholders. A well-designed and effective information campaign is not cheap. Developing content that describes risk without unnecessarily alarming people and without encouraging potential hackers requires careful planning.

  The European Commission will facilitate an exchange of best practice and ensure a certain level of co-ordination of the various national information campaigns at EU level, in particular as regards the substance of information to be provided. One element of this action would be a portal for web sites both at national and European level. Linking these portals to trusted web sites from international partners could also be envisaged.

- Member States should promote the use of best practice in security, based on existing measures such as ISO/IEC 17799 (code of practice for information security management www.iso.ch). Small and medium sized companies should be particularly targeted. The Commission will support Member States in their efforts.

- Education systems in Member States should give more emphasis on courses focused on security. The development of educational programs at all levels, for example training on the security risks of open networks and effective solutions should be encouraged to become part of computer education in schools.

  Teachers need in turn to learn about security in their own training programmes. The European Commission is supporting the development of new modules for the curricula in the context of its research programme

3.3. A European Warning and Information System

Even when users are aware of security risks they will still need to be alerted to new threats. Malicious attackers will almost inevitably find new vulnerabilities to circumvent state-of-the art protection. The industry is permanently developing new software applications and services, offering better quality of services, making the Internet more attractive, but in the process unintentionally opening up new vulnerabilities and risks.

Even experienced network engineers and security experts are often surprised by the novelty of some attacks. Therefore an early warning system is needed that can rapidly alert all users, together with a source of quick and trustworthy advice on how to tackle attacks. Business also needs a confidential mechanism to report attacks without risking to loose public confidence. This needs to be complemented by a more extensive forward-looking security analysis, bringing together evidence and assessing the risks with the benefit of a broader view.

Much work is done in this area by public and private "Computer Emergency Response Teams" (CERTs) or similar entities. For instance Belgium has established a virus alert system allowing Belgian citizens to be informed of virus threats within two hours. However CERTs operate differently in each Member State making co-operation complex. The existing CERTs are not always well equipped and their tasks are often not clearly defined. World-wide co-ordination is done through CERT/CC, which is part-funded by the US government and CERTs in Europe are dependent on the information release policy of CERT/CC and others.

As a result of these complexities European co-operation has so far been limited. Co-operation is essential to ensure early warning throughout the Union through the instantaneous exchange of information on the first signs of attack in one country. Therefore co-operation with the CERT system within the European Union should be strengthened as a matter of urgency. A first action aiming at strengthening the public/private co-operation on dependability of information infrastructures (including the development of early warning systems) and improving co-operation amongst CERTS has been agreed in the context of the *e*Europe action plan.

Proposed actions:

- Member States should review their CERT system with a view to strengthening the equipment and competence of existing CERTS. In support of national efforts the European Commission will develop a concrete proposal to strengthen co-operation within the European Union. This will include project proposals in the framework of the TEN Telecom program to ensure effective networking and the establishment of accompanying measures in the IST programme to facilitate exchange of information.

- Once the CERT network is established at EU-level it should be connected to similar institutions world wide, for example the proposed G8 incident reporting system.

- The Commission proposes to examine with Member States how to best organise at European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats. The organisational nature of a possible structure is a matter of discussion with the Member States.

3.4. Technology support

Investment in network and information security solutions is currently sub-optimal. This is the case both in terms of technology uptake and research into new solutions. In a context where emerging new technologies inevitably bring with them new risks, on-going research is vital.

Network and information security is already included in the Information Society Technologies (IST) Programme of the EU's 5th Framework Research Programme (representing €3.6 billion over four years), with approximately €30 million to be spent in collaborative research on security related technologies in 2001/2002.

Research at technical level on cryptography is well advanced in Europe. The Belgian algorithm called 'Rijndael' won the Advanced Encryption Standard competition organised by the US standardisation institute (NIST). The NESSIE (New European Schemes for Signature, Integrity and Encryption) IST-project has launched an enlarged competition on encryption algorithms fulfilling the requirements of new multimedia applications, mobile commerce and smart cards.

Proposed actions:

- The Commission is proposing to include security in the future 6th Framework programme, which is currently under discussion in Council and Parliament. For this spending to be optimal, it should be linked to a broader strategy for improved network and information security. Research supported by this program should address the key security challenges posed by the "all-digital" world and by the need to secure the rights of individuals and communities. It will focus on basic security mechanisms and their interoperability, dynamic security processes, advanced cryptography, privacy enhancement technologies, technologies to handle digital assets and technologies for dependability to support business and organisational functions in dynamic and mobile systems.

- Member States should actively promote the use of 'pluggable'[15] strong encryption products. Security solutions based on 'plug in encryption' must be available as an alternative to those embedded in operating systems.

3.5. Support for market oriented standardisation and certification

For security-enhancing solutions to be effective they have to be commonly implemented by relevant market players and preferably based on open international standards. One of the main barriers to the uptake of many security solutions, for instance electronic signatures, has been the lack of interoperability between different implementations. If two users wish to communicate securely across different environments interoperability must be ensured. The use of standardised protocols and interfaces should be encouraged, including the application of conformity testing as well as "interoperability" events. Open standards, preferably based on open source software may contribute to faster fault repair as well as greater transparency.

Also, information security evaluation contributes to the users' trust and confidence. The use of common criteria has facilitated mutual recognition as a method for evaluation in many countries [16] and these countries have also entered into an arrangement with the US and Canada for mutual recognition for IT security certificates.

Certification of business processes and information security management systems is supported by the European co-operation for accreditation (EA) [17]. Accreditation of certification bodies enhances confidence in their competence and impartiality, thus promoting the acceptance of their certificates throughout the Internal Market.

In addition to certification, interoperability tests should also be carried out. An example of this approach is the European Electronic Signatures Standardisation Initiative (EESSI), which is developing consensus solutions in support of the EU directive on electronic signatures. Other examples are the smart card initiative in *e*Europe and the Public Key Infrastructure (PKI) implementation initiatives launched within the Interchange of Data between Administration program (IDA).

There is no lack of standardisation efforts but a great number of competing standards and specifications that lead to fragmentation of the market and to non-interoperable solutions. Therefore current standardisation and certification activities need better co-ordination also to keep pace with the introduction of new security solutions. Harmonisation of specifications will lead to increased interoperability at the same time enabling swift implementation by market players.

Proposed actions:

- European standardisation organisations are invited to accelerate the work on interoperable and secure products and services within an ambitious and fixed timetable. Where necessary new forms of deliverables and procedures should be followed in order to speed up the work and to strengthen the co-operation with consumer representatives and the commitment from market players.

---

[15] 'Pluggable' means that an encryption software commodity can be easily installed and made fully operational on top of operating systems.

[16] Council Recommendation 95/144/EC on common information technology security evaluation criteria (implemented in the majority of EU Member States).

[17] European co-operation for Accreditation between accreditation bodies from 25 EU, EFTA and candidate countries.

- The Commission will continue to support, notably through the IST and IDA programs, the use of electronic signatures, the implementation of user friendly interoperable PKI solutions and the further deployment of IPv6 and IPSec [18](as provided for in the *e*Europe 2002 Action Plan).

- Member States are invited to promote the use of certification and accreditation procedures on generally accepted European and international standards favouring mutual recognition of certificates. The Commission will assess the need for a legal initiative on the mutual recognition of certificates before the end of 2001.

- European market players are encouraged to participate more actively in European (CEN, Cenelec, ETSI) and international standardisation activities (Internet Engineering Task Force (IETF) , World Wide Web Consortium (W3C)).

- Member States should review all relevant security standards. Competitions could be organised together with the Commission, for European encryption and security solutions with a view to stimulate internationally agreed standards.

3.6. Legal Framework

There are several legal texts influencing security in communication networks and information systems of which the regulatory framework for telecommunications is the most comprehensive. Because of the convergence of networks, security issues are now bringing together regulation and regulatory traditions from various sectors. These include **telecommunications** (encompassing all communication networks) which is being regulated and deregulated at the same time, the largely unregulated **computer industry** [19], the **Internet** which has functioned mainly on the basis of a 'hands off' approach and **e-commerce** which is increasingly subject to specific regulation. In relation to security, provisions regarding third-party liability, cyber-crime, electronic signatures, data protection and export regulations are relevant. Of these various provisions the data protection directives, the regulatory framework for telecommunications, and several legal initiatives in the context of the cyber-crime Communication are of particular relevance.

Protection of privacy is a key policy objective in the European Union. It was recognised as a basic right under Article 8 of the European Convention on human rights [20]. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union [21] also provide the right to respect for family and private life, home and communications and personal data.

The Data Protection Directives [22] and more particularly article 5 of the Telecommunications Data Protection Directive [23] oblige Member States to ensure the confidentiality in public

---

[18] IPv6 is an Internet protocol increasing the number of possible IP addresses, optimising the traffic routing of messages and enhancing the possibilities to deploy IPSec. IPSec is another Internet protocol aiming to provide confidentiality, to prevent packets from being viewed except by the receiving host and to provide authentication and integrity to guarantee that the data in the packet is authentic and from the correct sender.

[19] There are security requirements regarding electrical components of a computer, but no requirements as to security of data handled by a computer.

[20] http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm#HD_NM_15

[21] OJ C 364 of 18.12.2000, www.ue.eu.int/df/docs/en/CarteEN.pdf

[22] Directives 95/46/EC (OJ L281 of 23.11.1995) and 97/66/EC (OJ L24 of 30.1.1998) http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

[23] 'Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunication network and publicly available telecommunication services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with article 14 (1)'.

telecommunications networks, as well as publicly available telecommunication services. In addition, and in order to put article 5 into practice, under article 4 of the same Directive providers of public services and networks are required to take appropriate technical and organisational measures to safeguard the security of their services. In further accordance with the article, these measures must ensure a level of security that is appropriate to the risk presented, in view of the state of the art and the cost of their implementation. This means all network operators have a legal obligation to protect communications against unlawful interception. The pan-European nature of services and greater transborder competition will call for more harmonisation of these provisions.

The general Data Protection Directive 95/46/EC requires in article 17 controllers and processors to take measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected in particular if the processing involves the transmission of data over a network. They must implement appropriate technical and organisational measures against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.. These provisions have implications for security requirements on networks and information systems used by those persons and organisations for instance e-commerce service providers. The pan-European nature of services and greater transborder competition lead to increasing need for specification of the means to put in place in order to comply with these provisions.

The **EU framework for telecommunications services** contains several provisions with respect to 'security of network operations' (meaning availability of networks in case of emergency) and 'network integrity' (meaning ensuring normal operation of interconnected networks) [24]. The Commission proposed a new regulatory framework for electronic communication services in July 2000 (which is currently subject to the co-decision procedure and, therefore, discussed in the European Parliament and in the Council). The Commission proposals restate in essence - though with modifications - the existing provisions as regards network security and integrity.

The existing legal framework does, therefore, besides covering the specific topics addressed in each legal text, also concern certain aspects of networks and information systems as addressed by the present communication.

The **cyber-crime Communication** has triggered a debate in the European Union on how to react to criminal activities that use computers and electronic networks. Discussions will continue between all interested parties in the framework of the EU Forum to be set up shortly as announced in the Commission Communication on cyber-crime. Member States' criminal laws should cover unauthorised access to computer networks including the violation of personal data security. At present, there is no approximation of criminal law at the level of the European Union in this area. This can lead to problems investigating these offences and fails to provide a strong deterrent to those contemplating hacking or similar attacks. Approximation of criminal laws against intrusion into computer networks is also important to facilitate judicial co-operation between Member States.

The legitimate concerns about cyber-crime necessitate effective law enforcement investigations. However these legal concerns should not create solutions where legal requirements lead to weakening the security of communication and information systems.

[24] Commission Liberalisation Directive 90/388/EC, Interconnection Directive 97/33/EC, Voice Telephony Directive 98/10/EC.

Proposed actions:

- A common understanding of the legal implications of security in electronic communications is required. For this purpose the Commission will set up an inventory of national measures that have been taken in accordance with relevant Community law.
- Member States and the Commission should continue to support free circulation of encryption products and services through closer harmonisation of administrative export procedures and further relaxation of export controls.
- The Commission will propose a legislative measure under Title VI of the Treaty on the European Union to approximate national criminal laws relating to attacks against computer systems, including hacking and denial of service attacks. .

3.7. Security in government use

The *e*Europe 2002 Action Plan aims to encourage more effective and efficient interaction between citizens and the public administration. As much of the information exchanged between citizens and the administration is of a personal or confidential nature (medical, financial, legal etc.), security is vital to ensuring successful uptake. Furthermore, the development of e-government makes public administrations both potential **exemplars in demonstrating effective secure solutions** and market actors with the **ability to influence developments through their procurement decisions**.

The issue for public administrations is not just to procure information and communication technology systems with security requirements but to develop a culture of security in the organisation. This can be accomplished through the establishment of 'organisational security policies 'tailored to the needs of the institution.

Proposed actions:

- Member States should incorporate effective and interoperable information security solutions as a basic requirement in their e-government and e-procurement activities.
- Member States should introduce electronic signatures when offering online public services
- In the framework of the e-Commission, the Commission will take a series of measures to strengthen the security requirements in its information and communications systems.

3.8. International co-operation

Just as the communications using the networks easily cross borders in a fraction of a second, so do the associated security problems. The network is only as secure as the weakest link and Europe cannot isolate itself from the rest of the global network. Consequently addressing security issues require international co-operation.

The European Commission is already contributing to the work of international fora such as G8, OECD, UN. The private sector is dealing with security issues in their organisations such as the Global Business Dialogue (www.GBDe.org) or the Global Internet Project (www.GIP.org). A continuing dialogue between these organisations will be essential for global security.

Proposed action:

- The Commission will reinforce the dialogue with international organisations and partners on network security, and in particular on the increasing dependability on electronic networks.

4. Next steps

This Communication provides the strategic outline for action in this area. It is only a first step and not yet a definitive action plan for network security in Europe. However it already makes suggestions for actions in order to establish a framework for a common European approach. The next stage is for the framework and the proposed actions to be discussed by Member States and the European Parliament. The Göteborg European Council on 15/16 June may give orientations for the way ahead.

The Commission proposes to launch a thorough discussion with industry, users and data protection authorities on the practical details of implementing the actions proposed. Comments can be sent to eeurope@cec.eu.int by the end of August 2001. Therefore this Communication is an invitation for comments from interested parties with a view to establishing a final concrete set of actions. This could take the form of a roadmap to be developed by the end of 2001.

***