Chaillot Paper

March 2005

n°76

Information security

A new challenge for the EU

Alain Esterle, Hanno Ranck and Burkard Schmitt

Edited by Burkard Schmitt

Institute for Security Studies
Institut d'études de Sécurité
European Union
Union Européenne

In January 2002 the **Institute for Security Studies (ISS)** became an autonomous Paris-based agency of the European Union. Following an EU Council Joint Action of 20 July 2001, it is now an integral part of the new structures that will support the further development of the CFSP/ESDP. The Institute's core mission is to provide analyses and recommendations that can be of use and relevance to the formulation of the European security and defence policy. In carrying out that mission, it also acts as an interface between European experts and decision-makers at all levels.

Chaillot Papers are monographs on topical questions written either by a member of the ISS research team or by outside authors chosen and commissioned by the Institute. Early drafts are normally discussed at a seminar or study group of experts convened by the Institute and publication indicates that the paper is considered by the ISS as a useful and authoritative contribution to the debate on CFSP/ESDP. Responsibility for the views expressed in them lies exclusively with authors. *Chaillot Papers* are also accessible via the Institute's Website: **www.iss-eu.org**

Chaillot Paper

March 2005

n°76

Information security

A new challenge for the EU

Alain Esterle, Hanno Ranck and Burkard Schmitt
Edited by Burkard Schmitt

Institute for Security Studies
European Union
Paris

Institute for Security Studies
European Union
43 avenue du Président Wilson
75775 Paris cedex 16
tel.: +33 (0)1 56 89 19 30
fax: +33 (0)1 56 89 19 31
e-mail: institute@iss-eu.org
www.iss-eu.org

Director: Nicole Gnesotto

ISSN 1017-7566
ISBN 92-9198-069-2

Contents

n°76 March 2005

Préface

Nicole Gnesotto

Décrypter les relations complexes qui s'établissent entre la mondialisation économique et la sécurité internationale est sans doute l'une des tâches les plus urgentes et les plus ardues à l'ordre du jour des responsables européens. Le terrorisme international, par ses manifestations spectaculaires et ses connexions mondiales, constitue l'exemple le plus évident de cette relation. Mais la vulnérabilité des sociétés industrielles ne se limite pas aux risques d'attentats physiques contre les biens et les citoyens des pays cibles de la nébuleuse terroriste. Parce qu'elles sont en quelque sorte le moteur du processus de mondialisation, les technologies informatiques, et en particulier le réseau Internet, méritent une réflexion spécifique.

L'explosion des technologies informatiques affecte en effet considérablement la gestion de la sécurité internationale : au positif, elles permettent notamment l'émergence d'une société civile internationale dont l'influence le dispute parfois à celle des Etats. En négatif, elles créent d'immenses opportunités pour les réseaux et trafics de toutes sortes et peuvent surtout constituer des cibles majeures pour un « cyberterrorisme » dont les effets seraient dévastateurs sur l'ensemble des échanges des sociétés mondialisées. On se souvient déjà des déroutes, pourtant ponctuelles et vite maîtrisées, occasionnées dans différents pays par des pannes gigantesques du réseau électrique, ou encore des perturbations causées par l'introduction brutale de virus informatiques particulièrement performants. On imagine dès lors les ravages que pourrait causer une attaque terroriste ciblée contre l'Internet lui-même ou, via Internet, contre des infrastructures sensibles.

Cette réflexion sur les nouvelles dimensions de l'insécurité internationale fait partie des axes de travail prioritaires de l'Institut. Un précédent Cahier de Chaillot*, sous la plume de Gustav Lindstrom, avait inauguré cette série d'études sur ce que pourrait être une « homeland security » de l'Union européenne. D'autres publications, notamment sur la sécurité des infrastructures critiques, suivront. De façon tout aussi prospective, ce* Cahier de Chaillot*, rédigé sous la responsabilité de Burkard Schmitt, adjoint au directeur et spécialiste des questions d'armement au sein de l'Institut, explore les risques spécifiques aux systèmes informatiques et examine les réponses souhaitables au niveau de l'Union.*

Une telle publication pourra sembler technique à plus d'un lecteur. Son mérite tient pourtant dans la mise en lumière, de la façon la plus simple possible, des vulnérabilités multiples auquel est soumis l'outil le plus basique et le plus quotidien de la mondialisation : le système Internet. L'Union européenne est particulièrement vulnérable dans ce domaine, mais parti-

culièrement bien placée aussi pour constituer le niveau le plus adéquat pour la prévention et la gestion de ce type de risques informatiques. D'immenses enjeux industriels sont d'ailleurs à l'œuvre, s'agissant notamment du financement de la recherche et des technologies censées assurer la sécurité des systèmes d'information. D'ores et déjà, une certaine coopération a vu le jour entre les responsables de la sécurité de l'information au sein des vingt-cinq Etats membres. Tant il est vrai que la parade nationale, en ce domaine comme dans bien d'autres, relèverait aujourd'hui d'une grande illusion.

Paris, février 2005

Introduction

Since the invention of the wheel, technical innovations have driven the history of mankind. Some of them have been particularly important and have changed profoundly the way societies work and individuals live. The Internet is a perfect example of such an innovation. Based on common protocols to send electronic messages and identify machines, it has opened up a new area of communication and information, enabling us to transfer vast amounts of digital data for a great variety of applications within fractions of a second around the globe. Moving into the new domain of cyberspace, the Internet has overcome the barriers of distance and time, and is therefore rightly considered to be the symbol of globalisation.

Connectivity still differs greatly between continents, countries and social groups. However, in Western societies in particular, there is hardly an area that has not been affected by the 'Internet revolution'. Even those of us who do not go online to send e-mails, look up the latest news, book a hotel or buy a flight ticket, depend on the Internet because the society we live in increasingly depends on it.

Dependence, however, by definition creates vulnerabilities and risks. Thanks to its enormous success, the Internet has become the spinal column of our knowledge- and information-based society, and its (even temporary) disruption can cause major economic and financial damage.

But there is more to it than that. Almost all technologies can be used for the best and for the worst. This is particularly true of the Internet, which is by its very nature in a permanent and rapid state of change, open to everyone, multifunctional and transnational. All these features offer unique advantages, but they also play into the hands of wrongdoers and allow them to use the Internet for their own malicious purposes: the spread of illegal information, unauthorised access to sensitive data, electronic attacks on sensitive infrastructures, etc.

Cybercrime and cyberterrorism are particularly challenging for security planners, because the technical know-how and the tools for Internet misuse are both advancing and spreading rapidly. At the same time, the number of potential targets is enormous and keeps on growing. Last but not least, the traditional instruments used to fight wrongdoers, penal law and law enforcement, are still national domains, which makes it extremely difficult (to say the least) to cope with attacks that can be launched in total anonymity from any point on the globe.

This publication seeks to explain both aspects of this challenge: on the one hand, the security risks that the Internet implies and, on the other, the attempts of the EU and its member states to manage these risks.

In the first part, Hanno Ranck and Burkard Schmitt of the EUISS explain what the Internet is, how it works, and how it can be misused with malicious intent. Based on the experience of hacker attacks, they illustrate what politically motivated wrongdoers in particular could do and which tools they would have at their disposal to achieve their objectives. The authors present a technical rather than political assessment that is comprehensible to everyone. They have chosen this approach to achieve what is mostly needed in the fight against cyberattacks: awareness among Internet users that they run security risks as soon as they go online.

In the second part, Alain Esterle from the French Secrétariat général de la Défense nationale (SGDN) explains how Europe is trying to cope institutionally and politically with the challenges of information security (Infosec). He analyses different national approaches – which are mainly built on the tradition of intelligence communities – and the various EU activities in this field, which have a non-defence background and focus on the development of information societies.

In the conclusion, the authors suggest how the different national and EU approaches might be brought together into a common European Infosec policy, and what the focus of such a policy could or should be.

Threat assessment

Hanno Ranck and Burkard Schmitt

1

This chapter is neither a typical research paper nor a handbook for information technology (IT) experts. It is an attempt to explain, in simple terms, a technology and the various ways in which it can be used and misused.

Such an assessment of threats and risks is admittedly unconventional. In the specific case of the Internet, however, we are convinced that this is the most appropriate approach, because the behaviour of every single user is crucial for successful risk management. Of course, technical protection measures do matter and the expertise of IT specialists is indispensable. However, the danger of cyberattacks can be greatly reduced if Internet users know what the risks are and what should be done to avoid playing into the hands of wrongdoers.

The aim of this chapter is thus twofold: first, to create awareness among those who regularly use the Internet for professional reasons but who do not fully understand the risks that this involves; second, to foster sensibility among decision-makers that cyberspace is not only a domain for 'Internet freaks', but a unique area of technology that has both enormous potential and serious security challenges that we have to cope with.

To achieve these objectives, the chapter starts with a brief explanation of what the Internet is and how it works. This is vital for a better understanding of the risks and problems we face when we enter cyberspace. The following sections give an overview of what politically motivated wrongdoers, in particular, can actually do to use the Internet against us. Such an overview is by definition not exhaustive, but it illustrates where the main problems lie: the dissemination of disinformation, spying on confidential information and attacks against critical information systems. The conclusion sums up the main challenges and establishes a link to the political level, which will be dealt with in the second chapter.

The Internet

What it is

The Internet is a set of interconnected communications networks for the transfer of digital data. It is not owned or run by a specific company or institution, but functions as a worldwide collaboration between a great – and ever-growing – number of companies, institutions, research centres and commercial Internet Service Providers, who set up a network of networks.

The history of the Internet goes back to 1969, when several American universities succeeded for the first time to link four different computers to the so-called ARPANET. Based on this preparatory work, in 1973 the American Defence Advanced Research Projects Agency (DARPA) initiated a research programme to find common standards which would allow networked computers to communicate transparently across multiple linked networks. The result of this project was a system of protocols[1] known as the TCP/IP Protocol suite, named after the two initial protocols developed: Transmission Control Protocol (TCP) and Internet Protocol (IP). The TCP/IP protocol was a breakthrough in the development of the Internet, because it made it possible to interconnect different networks via so-called 'gateways'. The result was an open architecture of networks in which all data packages could be routed over every available path, achieving a maximum of redundancy[2] and speed.

Over the years, further protocols have been developed and added to the TCP/IP protocol suite. These protocols form a stack of four 'layers'. Each layer solves a set of problems involving the transmission of data. Protocols of the network layer, for example, are essential to get data from the source network to the destination network; protocols of the transport layer ensure that the data reaches the destination and arrives in the right order, they determine also which application the data is intended for. The application layer is where most common network programs and their corresponding protocols reside: Hypertext Transfer Protocol (HTTP – the World Wide Web), File Transport Protocol (FTP), Simple Mail Transfer Protocol (SMTP – e-mail) and many others.[3]

1. A protocol 'governs' communications between computers. It contains a formal description of message formats and the rules two computers must follow to exchange data.

2. 'Redundancy' means the provision of alternative paths to a destination.

3. *Wikipedia: The Free Encyclopedia*, 'Internet protocol suite'; http://en.wikipedia.org/wiki/TCP/IP, viewed 29 November 2004.

Internet Protocol Suite	
Application layer	HTTP, SMTP, FTP, SSH, IRC, SNMP
Transport layer	TCP, UDP, SCTP, RTP, DCCP
Network layer	IPv4, IPv6, ARP, IPX
Data link layer	Ethernet, 802.11 WiFi, Token ring, FDDI

Equally important for the success of the Internet was the development of HTML (hypertext markup language) by CERN in Geneva. This invention paved the way for the development of Mosaic, the first Internet browser based on a graphic user interface, which in turn has allowed even inexperienced computer users to access online information.

Computers can connect to the Internet either individually or as part of a so-called Local Area Network (LAN, see diagram in Annex 1). Every computer connected to the Internet becomes a part of it, and the data transferred via Internet can contain any kind of information and serve different purposes (e-mail, web-pages, Word-files, etc.).

Essential for the functioning of the Internet is the so-called 'domain name system' (DNS): to send and receive digital data via the net, a connected computer must be unmistakably recognised. This recognition is accomplished through the IP address, a unique identifying number assigned to every device (computer, router, server, firewall, printer, etc.) on the Internet. (For instance, the server[4] currently hosting the website of the EU Council is constantly identified by the IP address 194.7.121.11.)[5] However, since human brains are not made for storing complex numeric information, it is very difficult, to say the least, to use such long numbers. The DNS offers the solution to this problem: it is an enormous database, which is stored on numerous servers at different levels, and links IP addresses to so-called domain[6] names (for the Council website, the domain name is consilium.eu.int). Every time an Internet user types a domain name into the browser's address bar, he uses a DNS server to translate the human-readable domain name into a machine-readable IP address. The core of the DNS is made up of 13 root name servers (A.root to M.root) located in the United States (A, B, C, D, E, F, G, H, J, M), Sweden (I), United Kingdom (K) and Japan (L). These root servers are exact copies of one

4. A 'server' is a computer that is part of a network and provides services to the other computers in the network. It is dedicated to a specific role, such as processing name requests, hosting websites, sending or receiving e-mails, etc.

5. If a single computer connects via an ISP, it will normally not be given a permanent IP address, as the number of possible addresses is limited to 256^4 and most of these are already reserved for special purposes. It will instead be assigned a temporary IP address valid only for the duration of the session.

6. A 'domain' is a 'logical' region of the Internet. In general, a domain corresponds to an IP address and/or a space on a server.

another and store information about all generic (.com, .org, .net...) and country-code (.de, .fr, .co.uk...) top-level domains.

Initiated in the United States as a defence-oriented research project, the Internet rapidly expanded internationally. At first it mainly involved research centres and universities, and then began to include more and more commercial facilities. By the end of 1991, it had grown to include some 5,000 networks in 40 countries, serving over 700,000 host computers;[7] by the mid-1990s, the Internet had connected more than 18,000 private and public networks with 3,200,000 'hosts'; in 1998, the Internet served about 35,000,000 host computers worldwide. In parallel, the number of Internet users exploded from some 4,000,000 in 1991 to more than 812,000,000 in 2004, and is still increasing.

World Internet Usage and Population Statistics[8]

World regions	Population (2004 est.)	Internet usage, (Year 2000)	Internet usage, latest data 2004	User growth (percentage 2000-2004)	Penetration (percentage of population)	Percentage of world
Africa	893,197,200	4,514,400	**12,937,100**	186.6	1.4	1.6
Asia	3,607,499,800	114,303,000	**257,898,314**	125.6	7.1	31.7
Europe	730,894,078	103,096,093	**230,886,424**	124.0	31.6	28.4
Middle East	258,993,600	5,284,800	**17,325,900**	227.8	6.7	2.1
North America	325,246,100	108,096,800	**222,165,659**	105.5	68.3	27.3
Latin America/ Caribbean	541,775,800	18,068,919	**55,930,974**	209.5	10.3	6.9
Oceania	32,540,909	7,619,500	**15,787,221**	107.2	48.5	1.9
WORLD TOTAL	6,390,147,487	360,983,512	**812,931,592**	125.2	12.7	100.0

NOTES: (1) Internet usage and population statistics were updated on 30 September 2004. (2) For detailed regional data, click on each World Region. (3) Demographic (population) numbers are based on data contained in the web site gazetteer.de. (4) Internet usage information comes from data published by Nielsen//NetRatings, by International Telecommunications Union, by NICs and other reliable sources. (5) Data from this site may be cited, giving the due credit and establishing an active link back to InternetWorldStats.com. (6) For navigation help and definitions, see the Site Surfing Guide.

The bulk of the system today is made up of networking facilities in educational and research institutions, business and government organisations around the globe. However, by far the biggest part of the Internet infrastructure (about 95 per cent) is now owned by private business, in particular telecommunication companies and commercial Internet service providers (ISPs).

The main responsibility for the stable and secure operation of the Internet lies with the Internet Corporation for Assigned Names and Numbers (ICANN),[10] a private, non-profit technical coordination body. ICANN is a 'cross-stakeholder, self-regulatory

7. A 'host' is a computer that provides services to other computers, e.g. mail, file or print servers. A client, in contrast, is a computer that requests services from another computer. Since clients can have access to the Internet as well, the number of computers connected to the Internet – and even more so the number of Internet users – has always been much higher than the number of hosts.

8. 'Internet World Stats: Usage and Population Statistics'; http://www.internetworldstats.com/stats2.htm, viewed 29 November 2004.

9. Conference on 18 October 2001 on 'Strengthening Homeland Cyber Defence', Center for Strategic and International Studies (CSIS) and the Information Technology Association of America (ITAA), Washington DC, October 2004, (Conference Summary); http://www.csis.org/tech/events/011018event/, viewed 29 November 2004.

10. ICANN was established in November 1998 to take over the functions of the Internet Assigned Numbers Authority (IANA), which was closely related to the US government; http://www.icann.org/ general/icann-mou-25nov98. htm, viewed 29 November 2004.

mechanism'[11] that administers, in particular, the distribution of IP addresses and domain names, ensuring that every IP address is unique and that each domain name corresponds to the correct IP address. It oversees the deployment of the DNS root servers and is responsible for populating all generic and country code top-level domains. Furthermore, ICANN is involved in the coordination of protocol parameter assignment for the TCP/IP protocol suite and the allocation of global address space to each of the four Regional Internet Registries (North America, Latin and Central America, Asia/Pacific, Europe), which in turn assign network Internet addresses to network operators.[12]

The risks

The Internet has become an integral part of our daily private and (even more so) professional life. In Western societies in particular, it is today one of the key means for communicating and accessing information. Moreover, and in spite of the Internet bubble bursting in 2001-02, it represents an enormously important economic factor.[13] E-commerce and online banking, for example, continue to experience annual two-digit growth rates, in both the United States and the EU (in particular in the Nordic countries).[14] At the same time, public services increasingly use the Internet to communicate both with each other and with citizens (e-government, eEurope[15]).

Accessible from (almost) everywhere by a variety of means, the Internet is a tool available to (almost) everyone, to fulfil a broad range of purposes at low cost and high speed. It is therefore not astonishing that an ever-growing number of individuals, companies, organisations and institutions use it and rely on it. However, the increasing interconnectivity and the success of the Internet also create new dependency.[16] Dependency by definition creates vulnerabilities, and the open architecture of the Internet is not only its biggest advantage, it also opens the door to possible misuse. For the academic community that developed the Internet protocol suite, security meant mainly survivability of the network against attacks on its infrastructure. That is why most of the Internet protocols do not fulfil security conditions (such as authentication and confidentiality), which are crucial for Internet services. As a result, the multifunctionality and ever-growing importance of the Internet raise now serious security questions, in particular

11. Vinton G. Cerf., presentation on 'Internet Governance', ICANN, 28 October 2004; http://www.icann.org/presentations/cerf-internet-publication-28oct04.pdf, viewed 29 November 2004.

12. The four Regional Internet Registries are the North American Registry for Internet Numbers (ARIN), Latin and Central American Network Information Center (LACNIC), Asia/Pacific Network Information Center (APNIC), and the Réseau Internet Protocol Européen Network (Coordination Centre) (RIPE-NCC); http://www.icann.org.

13. The Internet Economy Indicators, 'Dot Coms and Productivity in the Internet Economy'; http://www.internetindicators.com/prod_rept.html, viewed 29 November 2004.

14. Marketing Vox, 'E-Commerce Sees Late Growth Sprint', 19 October 2004; , viewed 29 November 2004. Nua Internet Surveys, 'Datamonitor: Europe's online banking population to rise', 28 March 2003; http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905358751&rel=true, viewed 29 November 2004. SEO-Strategy.org; http://www.seo-strategy.org/seo-articles/ecommerce.html, viewed 29 November 2004.

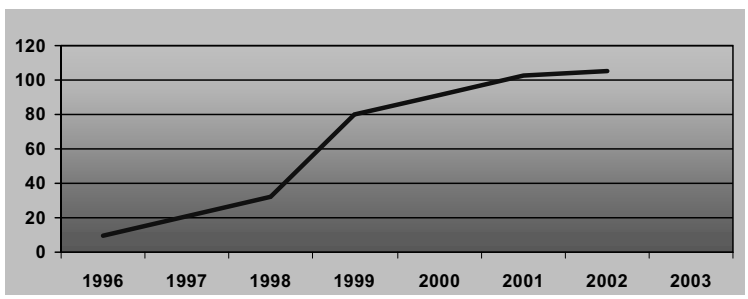
15. DG Information Society, eEurope 2005; http://europa.eu.int/information_society/eeurope/2005/index_en.htm, viewed 29 November 2004.

16. B. Nelson, R. Choi, M. Lacobucci, M. Mitchell and G. Gagnon, 'Cyberterror: Prospects and Implications', White Paper prepared for Defense Intelligence Agency and Office for Counterterrorism Analysis, Monterey, Calif., Center for the Study of Terrorism and Irregular Warfare, October 1999; http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf, viewed 29 November 2004.

since numerous LANs, including those of services that are vital for the functioning of our society, are connected to it.

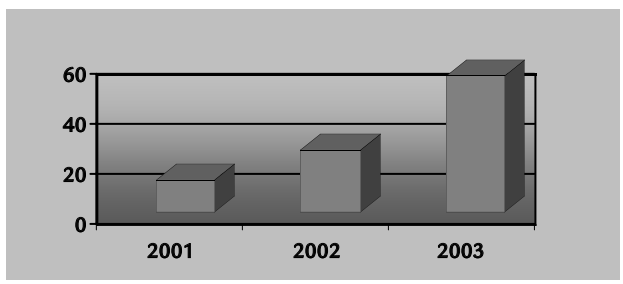
All users are familiar with the constant threat of viruses and worms that clog the Internet. The number of virus and worm attacks has exploded over the last few years, and they have become increasingly sophisticated. The necessary hacker tools are easily available online, and there is a constant exchange of information and know-how within the hacker community to make these attacks ever more efficient. The basic motivation of hackers, however, is 'only' to demonstrate their performance and power to a wider public and other hackers. The economic damage is nevertheless enormous. In 2004, for example, the three viruses Bagle, MyDoom and NetSky together caused damage amounting to more than $100 billion worldwide within less than three months.[17]

Virus infections per 1,000 computers



Source: http://infosecuritymag.techtarget.com

Damage caused by viruses in $billion



Source: ZDNet Security News Article 11/2004

17. 'Economic damage from Bagle, MyDoom, & NetSky crosses $100bn; Financial motive behind the malware variants likely', mi2g, 8 March 2004; http://www.mi2g.com/cgi/mi2g/press/080304.php, viewed 29 November 2004.

But the Internet is more than just the playground of hackers. All kinds of wrongdoers can exploit the Web for their own malicious purposes, and they increasingly do so. Given its advantages and multiple applications, it is hardly surprising that criminal and terrorist organisations, in particular, have discovered the Internet as a tool to pursue their objectives.

Broadly speaking, malefactors can use the web to:

- communicate and spread (dis)information;
- spy on others' information and communications;
- attack related networks and information systems; and
- target the Internet itself.

The number of criminal online activities has grown in parallel with the economic importance of the Internet. The banking sector in particular has become a prime target for online fraud, resulting in billions of euros of costs for both banks and users each year. In contrast, there has never been – at least officially – a major, politically motivated cyberattack against the Internet or related information systems. However, this does not mean that such an attack will never happen. Terrorist networks already use the Internet widely as an information and communication tool, and the more the fight against terror cuts traditional communication channels, the more attractive they find the Internet's accessibility and anonymity. At the same time, public authorities, particularly in the United States, have developed their own tools and strategies to counter these threats. The Internet has thus become the arena of a permanent online battle between hackers, criminals and terrorist organisations, on the one hand, and police and intelligence services on the other. Ordinary Internet users who are not aware of this can easily get caught between the frontlines and fall victim to it.

Circulation of illegal or dangerous information

Websites

Websites are ideal tools for disseminating information (and disinformation) on a global scale. Terrorist groups therefore increasingly use them for their propaganda, and the way they do so is becoming more and more professional and adapted to be effective in the media.[18] Moreover, terrorist organisations use websites for

18. G. Weimann, 'www.terror.net: How modern terrorism uses the Internet', USIP *Special Report* 116, March 2004; http://www.usip.org/pubs/specialreports/sr116.pdf, viewed 29 November 2004.

the recruitment of new members and for indoctrination and instruction of existing members.[19]

One of the first terrorist organisations to exploit the Internet as a propaganda tool was the LTTE (Liberation Tigers of Tamil Eelam, commonly known as the Tamil Tigers) of Sri Lanka.[20] Today, groups such as Hamas, Hezbollah, the People's Mujaheddin, the Kurdish PKK, al-Qaeda, Ansar al-Islam, Hizb-ul Mujaheddin (Kashmir), ETA or the IRA all have a presence on the World Wide Web, which illustrates the global nature of both the terrorist threat and the Internet as a tool.[21]

For terrorist groups, websites offer plenty of advantages. First, they are easy to build and use. It is not necessary to have enhanced technical skills or programming knowledge to create at least a basic information site, and software providing standardised templates makes it possible, even for total beginners, to disseminate information via the web.

The second advantage is accessibility. Websites can be uploaded (and consulted) from every point on the planet through a variety of means, and many Internet providers even offer webspace to host Internet sites free.[22]

The third advantage is anonymity: anyone can connect to a commercial Internet provider and upload a website without valid registration. Cost-free Internet providers and unprotected wireless LAN 'hot spots',[23] in particular, do not require proper user authentication and therefore provide perfect anonymity. Moreover, once the site is online, it is technically close to impossible to trace the exact upload source location.[24]

An alternative strategy for wrongdoers is not to upload websites on their own domains, but to 'capture' other well-frequented websites. Users will then find the website of the wrongdoer when they type in the domain name of the site they initially wanted to visit. In the United States, hackers have in the past succeeded in capturing and falsifying federal websites such as those of the Department of Justice, the United States Air Force, CIA, or NASA.[25] This illustrates that even highly secure domains can fall victim to such attacks. Capturing websites is particularly effective for the dissemination of multimedia files. It will not normally take the domain owner very long to detect and stop the fraud, but even during a short time thousands of users can visit the captured website and see the information displayed on it. One can fairly assume that this is sufficient, for example for a video to find its way into

19. Ibid.

20. Shyman Tekwani, 'The LTTE's Online Network and its Implications for Regional Security', Non Traditional Security in Asia, Nanyang Technological University, Singapore; http://www.idss-nts.org/PDF/Shyman%20Tekwani.pdf, viewed 29 November 2004.

21. Ibid.; G. Weimann, 'OP-ED: Terrorism and the Internet', 30 April 2004; http://www.daily-times.com.pk/default.asp?page=story_30-4-2004_pg3_5, viewed 29 November 2004.

22. However, cost-free ISPs normally offer only very limited web space and low-speed access, which means that they can only host very simple websites.

23. Many access points to (mostly commercial) wireless Internet connections are not – or not sufficiently –protected, so that everyone who is within the range of the radio signal can use it.

24. See Peterson, Gallagher, Borchgraze, Cillusso, S. Lanz, Berkowitz, and William H. Webster, 'Cybercrime, Cyberterrorism, Cyberwarfare: Averting an electronic Waterloo', CSIS *Task Force Report*, Washington, DC, Center for Strategic and International Studies, 1 June 1998.

25. *St Petersburg Times*, http://www.sptimes.com/Hackers/history.hacking.html.

peer-to-peer-networks (see below), which will then make it impossible to stop its duplication and distribution.

Another variety of domain capturing was used by the webmaster of AlNeda.com, a website that served as a propaganda instrument for al-Qaeda.[26] Once the website had been banned from all commercial service providers, the webmaster hacked into web servers and inserted his files illegally into others' websites. The AlNeda website was then accessible under covert Internet addresses, which were posted on other Islamic sites, but could also be found on search engines operating in Arabic.[27]

All this illustrates how difficult it is to deny wrongdoers the use of the World Wide Web as a platform. Public authorities today use modern 'spider' and search engine technologies to scan the entire Internet for critical websites, and they can also force commercial Internet providers to ban illegal sites. However, given the global nature of the Internet and the continuously growing number of ISPs worldwide, national law enforcement services may be able to limit the use of such websites, but they will hardly be able to ban them completely.

E-mail

Electronic mail has become one of the most important forms of communication in the world. According to IDC, the number of e-mails sent worldwide is expected to grow from 15.5 billion daily in 2001 to 35 billion daily in 2006.[28] The reasons for the success of e-mails are well known: they are cheap, fast and can be used to send any kind of multimedia content as an attachment. Two other characteristics, anonymity and accessibility, are again particularly advantageous for wrongdoers: the sender of an e-mail does not have to reveal his identity, the technical possibilities to trace e-mails are limited, and Internet cafés are perfect launch pads for anonymous dissemination. A new e-mail address is created in about three minutes – certainly cost-free and without the need for any valid identification. All this makes e-mail a perfect communication tool for wrongdoers. Since the war in Afghanistan, for example, electronic mailing has become one of al-Qaeda's main tools for re-establishing links between its various cells.[29]

On top of that, wrongdoers can also misuse the 'marketing ploy' of mass e-mailing. Information and disinformation can easily be multiplied by thousands and reach your mailbox. Moreover,

26. In summer 2002, a private hacker based in Maryland (United States) took over the domain name of the alNeda website. When the owners of alneda.com had to delete its registration from an ISP in Kuala Lumpur (apparently due to pressure from the US government), the hacker used the short moment before the site was registered on another ISP to sign on its own domain with the same name. He was then listed as the owner of alNeda.com. He uploaded a copy of the original alNeda website on his domain and added a tracking software. Visitors first believed www.alneda.com was still the real al-Qaeda site, which allowed the hacker to trace many Islamic message boards and websites on the Internet. After five days, a message was posted on an Islamic message board by the person who had regularly maintained the actual alNeda website, saying that the 'infidels were tracking information and that users should stay away'. With his cover blown, the hacker replaced the website with a picture of the Great Seal of the United States and the phrase, 'Hacked, tracked and now owned by the USA'. That same morning, the real alNeda website appeared temporarily at http://www.news4arab.org, which has since gone down. See http://www.wired.com/news/culture/0,1284,54455,00.html?tw=wn_story_page_prev2.

27. See Scott Shane, 'The Web as al-Qaida's Safety Net', *The Baltimore Sun*, 28 March 2003. The article is also available in the *Chicago Tribune*, 2 April 2003, at http://www.chicagotribune.com/technology/chi-0402alqaida,0,1984424.story?coll=chi-technology-hed, viewed 29 November 2004.

28. Shyman Tekwani, 'The LTTE's Online Network and its Implications for Regional Security', Non Traditional Security in Asia, Nanyang Technological University, Singapore; http://www.idss-nts.org/PDF/Shyman%20Tekwani.pdf, viewed 29 November 2004.

29. James Risen and David Johnston, 'A Nation Challenged: The

user IDs and passwords can be captured and misused. In 1997, for example, LTTE hacked into the e-mail server of Sheffield University, hijacked the IDs of some well-respected academics and misused their e-mails to distribute propaganda and engage in fundraising.[30] Last but not least, e-mail can also be used as a transport medium for cyberattacks (see the section on destruction and obstruction of critical information systems below).

A particularly perfidious way of using e-mails with malicious intent is e-mail spoofing. In this case, a wrongdoer uses the e-mail address of an unsuspecting third party to send a mail, often with a hidden dangerous payload (such as a virus). He can do so, for instance, by exploiting a weakness of the so-called Simple Mail Transfer Protocol (SMTP), a server-to-server protocol, which is part of the TCP/IP suite and controls how e-mail is sent via Internet. In its basic version, SMTP has no authentication procedure and therefore cannot verify the identity of the sender. The wrongdoer can thus easily send e-mail with sender names of his own choice if he uses one of the many SMTP servers that work with this SMTP version.

Spying on confidential information

Hacking and computer break-in

Every computer system connected to a network is vulnerable to intrusion, and all digital information stored on it risks being tapped by intruders. Whether data is spied on by a business competitor, a foreign secret service, a terrorist or just by 'ordinary' hackers, in most cases the victim will either not even realise that his computer has been hacked and information copied by a third party or, when he does, it will be too late to react.

The most widespread tools for computer-break-ins are 'Trojan horses' or 'backdoors'. Hidden as apparently harmless and/or useful content, they are either sent via e-mail or hidden behind hyperlinks. If a user opens the attachment or clicks on the hyperlink, the Trojan horse will inwardly open a trap door into the relevant security protection settings of his computer. Through this door, the attacker can access the victim's computer and do virtually anything he wants: copy, change, destroy or send all kinds of files (whether they are confidential or not), send falsified e-mails,

Terrorist; Al Qaeda May Be Rebuilding in Pakistan, E-Mails Indicate', *New York Times*, 6 March 2002.

30. Tekwani, op. cit. in note 28.

access the local area network to which the victim's computer may be connected, or use the computer as part of a DDoS attack (see below).

One of the major problems in this context is the rapid spread of the know-how needed for such attacks. The tools for computer break-ins are (relatively) easy to obtain. Specialised hacker sites provide information on where to find and how to use the necessary software. Using peer-to-peer networks, which establish a direct connection between two computers, wrongdoers can find and exchange almost all kinds of illegal software. The software necessary to get access to the search engines of such peer-to-peer networks is available for everybody, legally and cost-free, although it is well known that these networks are used mainly for the exchange of illegal software.[31]

Companies as well as public services spend enormous sums on protection against hackers and computer espionage, but even highly sensitive governmental systems have proved to be vulnerable. Operation *Eligible Receiver*, organised in 1997 by the NSA, revealed major security breaches in US military networks. A 35-strong team was instructed to prove their ability to spy on and disrupt the networks of the Pacific Command in Hawaii using only hacker tools available on the Internet. The team was able to break through network defences untraced, after which they could have spied, changed or spoofed sensitive e-mails, disrupted telephone service, etc.[32]

Certainly these security gaps have since been closed and the overall protection of governmental institutions has improved dramatically. But one has to be realistic: a specialised team of hackers with the capability to programme their own tools, certain financial resources and sophisticated technical equipment, could probably pose a major threat to sensitive governmental networks.[33] In 1999, for example, over a period of several months hackers operating from as many as 15 locations worldwide launched up to 100 coordinated attacks per day on Pentagon computers. Among the computers targeted were those of the Air Intelligence Agency, the Air Force Information Warfare Center and a Joint Chiefs of Staff command-and-control operation. In spite of the lessons learned from Operation *Eligible Receiver* two years earlier, some of these attacks succeeded in penetrating defences: in particular, hackers repeatedly tapped into military computers at Kelly Air Force Base in San Antonio – the centre of the most sensitive Air Force

31. The software which gives access to these networks is difficult to inhibit since operating companies put (a) a disclaimer on their websites reminding users to exchange only legal, copyright free content and (b) deny any further responsibility by an escape clause.

32. Gabriel Weimann, 'Cyberterrorism: How real is the threat?', *Special Report* 119, United States Institute of Peace, Washington, DC, May 2004; http://www.usip.org/pubs/specialreports/sr119.html, viewed 29 November 2004.

33. White Paper prepared for Defense Intelligence Agency and Office for Counterterrorism Analysis, op. cit. in note 16.

intelligence, critical to American troops who were at the time on patrol over Iraq and in Bosnia.[34]

Internet and e-mail interception

All data transfers via Internet runs the risk of interception, and there are different ways of spying on electronically transmitted information. The most famous espionage system is Echelon, a system dominated by the NSA and financed by the United States, United Kingdom, Australia, New Zealand and Canada.[35] Echelon was created during the Cold War for military purposes, but is suspected of intercepting all kinds of 'relevant' communications worldwide, including private and commercial ones. It can spy on satellite communications, in particular telecommunications, but also Internet traffic that is routed via satellite. One of its key components consists of the so-called 'dictionary computers', which filter all passing data traffic for keywords (topics, names, telephone numbers)[36] and forward all matches to the NSA for further analysis. However, as a tool for Internet espionage, Echelon is becoming less important. First, the increasing use of encryption for the transfer of sensitive data is rendering the dictionary computers ineffective. Second, Echelon is set up for electromagnetic signals, and cannot scan fibre optics. The latter, however, are increasingly replacing satellites for Internet traffic, because they allow for higher and faster data transfer.

However, the use of fibre optics is no guarantee against interception. Internet data packages are routed through various networks and servers; the request for a website can easily pass 30 or more hosts before arriving at the final server destination, and e-mail is routed in a very similar way. On its way, the information can be intercepted by a third party – both inside and outside the LAN of the sender and the receiver – with the help of so-called 'packet sniffers'.

A packet sniffer is a software program that scans the flow of information through a network. Normally a computer reacts exclusively to data packages that contain information for its own IP address. A packet sniffer, in contrast, can be set up to control data flow from or to various selected IP addresses, or even the entire data traffic on the network. Some packet sniffers also react to certain keywords. They copy all e-mails sent and received that fulfil the defined search criteria, and record which websites are

34. Zdnet.com, 'Pentagon and hackers in "cyberwar"', MSNBC, 4 March 1999; http://zdnet.com.com/2100-11-513930.html, viewed 29 November 2004.

35. The existence of Echelon was revealed in 1997 by a STOA (Scientific and Technological Options Assessment) Task Force and corroborated by a European Parliament resolution (2001/2098 (INI)). See: 'An Appraisal of Technologies of Political Control' from the Omega Foundation for the European Parliament in 1997, Report commissioned by STOA; European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system) (2001/2098(INI)), *Official Journal of the European Communities*, C 72 E/221, 21 March 2002.

36. See Duncan Campbell, 'Interception Capabilities 2000: Report to the Director General for Research of the European Parliament on the development of surveillance technology and risk of abuse of economic information', IPTV Ltd, Edinburgh, April 1999, p. 17; http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm, viewed 29 November 2004.

accessed from the respective IP addresses. Packet sniffers can also be used to capture user passwords or to spy on instant message communication.

Much sniffer software is easily and legally available on the market, commercialised in general as systems for the detection of suspicious data traffic on local area networks. However, the capacity to keep a LAN under surveillance can easily be misused to control all Internet and Intranet communication of the members of that LAN.[37] Moreover, packet sniffers can also be installed in a LAN from the outside by a third party. If a wrongdoer succeeded in penetrating a LAN, for example with the help of a Trojan horse, he could instal malicious software on any computer connected to the LAN and monitor the entire network through a manipulation of the switch.[38]

To use packet sniffers for the surveillance of Internet service providers (where the amount of traffic is of course much higher) is more difficult. First, ISPs are usually well protected against intrusion. Second, most commercially available packet sniffers can only work on one subnet at a time,[39] whereas an ISP routes data packets of computers from several subnets. However, some intelligence services have developed their own, much more sophisticated sniffer programs that are able to cope with this. If installed at an ISP or other Internet key distribution points, these sniffers can filter all kinds of data, read any passing message and note which websites are consulted. An example of such high-performance sniffer programs is DCS1000 (*Carnivore*), which is used by the FBI to carry out targeted surveillance of criminal suspects.[40]

Destruction and disruption of critical information systems

In almost all areas, our complex societies increasingly depend on systems that store and process digital information.[41] Hacker attacks repeatedly illustrate the vulnerability of these information systems and the potential damage that destruction or disruption of the latter could cause. Whereas most hackers aim to demonstrate their capacity to destroy rather than actually to destroy, other wrongdoers could follow the opposite logic. The threat of politically motivated attacks aimed at the destruction or disruption of critical information systems has therefore become a major concern of security planners. Up until today,

37. See 'Customers' pick on this website; http://www.effetech.com/.

38 A 'switch' is a connectivity point on a network. It knows the protocols and learns which device is connected to which of its ports and how it is used. It will therefore by default not transmit the packet to every node of the network, but only to the one concerned. The intruder will try to fool the switch into broadcasting to a device it is not supposed to. If distribution in the network is based on a hub, this manipulation is not even needed, since it will always broadcast.

39. A subnet is a group of nodes which have IP addresses that are logically one network (for example 192.168.10.1-192.168.10.255).

40. See Dr Franz Büllingen and Annette Hillebrand, 'Rechtlicher Rahmen für das Angebot von TK-Diensten und den Betrieb von TK-Anlagen in den G7-Staaten in Bezug auf die Sicherstellung der Überwachbarkeit. im Auftrag des Bundesministeriums für Wirtschaft und Arbeit der Telekommunikation', p. 64; http://www.bmwa.bund.de/Redaktion/Inhalte/Pdf/Homepage_2Fdownload_2Ftelekommunikation__post_2FTKUEG7.pdf,property=pdf.pdf.

41. A. de Borchgrave, F. Cilluffo, S. Cardash, and M. Ledgerwood, *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, (Washington, DC: Center for Strategic and International Studies Press, May 2001), p. 9; http://www.csis.org/pubs/2001_cyberthreatsandis.htm.

cyberterrorism has never developed into a major attack. The destructive potential, however, is great. Information warfare specialists have estimated that a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos strategically located around the world, with a budget of less than $10 million, could cause an 'economical Waterloo' and bring the United States to its knees.[42]

Cyberterrorists can target the Internet itself, but they can also use the Internet as a gateway to penetrate and attack local area networks (and their host computers). Physical separation of the LAN from the Internet, so-called 'air gaps', offers the best protection, but is only a realistic option in exceptional cases. First, air gaps are expensive, because twice as many computers are necessary in order to have the same degree of connectivity. Second, air gaps provide absolute security only if not a single file received via the Internet is processed on computers connected to the LAN – which is hardly practicable. Most institutions and companies, therefore, prefer to use firewalls and virus scanners to protect their networks against cyberattacks. However, even the best firewall can only reduce the risk; it will not be able to eliminate it completely. This is particularly problematic where information systems of critical infrastructures are concerned.

DDoS

Experience with hack–attacks shows that one of the most effective ways to obstruct critical information systems is a distributed denial of service (DDoS) attack. In such an attack, the hacker initially breaks into computers, often with Trojan horses, and installs a 'daemon' (a kind of virus) in them. At a later point, he sends a request to the daemon on the compromised computers asking it to begin flooding a target with various types of data packets. The ensuing massive stream of data overwhelms the victim's hosts or routers, rendering them incapable of providing service.

There are different forms of DDoS attacks; some only target the bandwidth through repeated 'ping'[43] floods, whereas others are more intelligent and ask a server to connect to a large number of IP addresses created by a random algorithm. Many of the spoofed IP addresses will not answer, because they do not represent an available node, so that the waiting list on the target server fills up until it refuses any kind of new request – even valid ones.

42. W. Judge, H. Webster and A. de Borchgrave, 'Cyberterrorism and cyberwarfare thus become a plausible alternative', Computer Crime Research Center (CCRC); http://www.crime-research.org/library/Judge.htm, viewed 29 November 2004.

43. Packet Internet Groper is a utility used to determine whether a specific computer is currently connected to the Internet. It works by sending a packet to the specified IP address and waiting for a reply.

Amplifier attacks like 'smurf' or 'fraggle' use the distribution function of IP broadcast addresses.[44] On a multi-access broadcast network of, for example an ISP, there could potentially be hundreds of nodes to reply to each data packet sent by the compromised computers. All varieties of DDoS attacks have in common that they cause some kind of 'overload', which does not damage the target machine physically, but disables it for the duration of the attack.

DDoS attacks can affect single devices such as web hosting servers, DNS servers or routers, but they can also bring entire networks down. Given their importance for the functioning of the Internet, root DNS servers are certainly among the most attractive targets. On 23 October 2002, a massive DDoS attack struck down nine of the thirteen DNS root servers. The actual impact of the carefully concerted attack on the web was minimal. But what would have happened if it had been not nine but eleven root servers, which were unable to cope with the ping flooding? Theoretically, the Internet could still work with only one or two root servers, but the number of requests would be so big that most of them would not be answered.

But DDoS is not only a danger to the DNS. A political motivated cyberattack could also target the networks of sensitive infrastructures and/or public services. Frequently visited websites and ISPs can be attractive targets as well, particularly for attackers who want to damage a specific company or seek maximal visibility. In October 2004, for example, a DDoS attack brought down the official website of the George W. Bush electoral campaign for two days. Only one week before the elections, there was enormous pressure to remake – and keep – the site accessible. Once the site was online again, the Webmaster denied access to all users outside the United States.[45] This response, however, was totally insufficient, since the site remained accessible from everywhere via its IP address: 65.172.163.222.[46]

This episode illustrates perfectly how effective DDoS attacks can be, particularly if they are well timed. In many cases it is very hard to defend against them, because the attacking computers are not the computers of the wrongdoers but only the ones infected with a daemon which unwittingly makes it part of the DDoS attack. Even the filtering of the malicious IP addresses can be difficult if they are spoofed and change rapidly.

44. A broadcast is a data packet destined for all nodes on a particular network; IP broadcast addresses are used for delivering single data packets within LANs from a host to every node with an IP address connected to that LAN.

45. 'Vollsperrung für den Rest der Welt', *Spiegel Online*, 28 October 2004; http://www.spiegel.de.

46. Since then, the IP address has changed. On 1 March 2005 the site was accessible under 64.203.98.31.

Virus and worm attacks

Computer viruses and worms are both malicious codes, but they replicate and spread in different ways. Viruses mainly use file exchange and boot sectors to spread,[47] worms spread via network environments and e-mail. Worms are self-contained programs that replicate themselves, whereas viruses infect certain types of data files, in particular files that support executable content (.exe, .com, .pif, etc.) and files that rely on macros (.doc, .xls, etc.). Every infected file itself acts as a virus and can infect other files. Depending on the programming of the virus, the computer itself can initiate the necessary execution of the file automatically (for example in the boot process at system start-up) or the user himself may do it unintentionally (by a specific manipulation of his computer).

In most cases, the virus or worm itself is not the real problem. The infected computer might slow down a little when the malicious code claims system resources to copy itself, but normally this process is not even apparent to the user of the infected computer. However, while the first task of both virus and worm is self-replication and distribution, they can also have a payload, which can fulfil any kind of purpose: it can change files, render them unserviceable or completely delete them. In 1998, for instance, the CIH virus disabled thousands of computers. The payload was to destroy the BIOS information,[48] rendering the system unbootable. In April 2000, Love Letter, a VBScript worm, was spread via e-mails, which were sent as a chain letter. Love Letter also deployed a malicious payload as part of its routine, overwriting certain media file types. The worm affected millions of computer systems around the world and crippled e-mail systems, for example in the British Parliament and the Pentagon.[49] Since early 2004, Bagle, Mydoom and Netsky have flooded e-mail systems worldwide. Programmed for the Windows 32 environment, these worms are particularly effective because they send themselves autonomously via e-mails that constantly change their appearance.[50] None of these attacks has been politically motivated, but their destructiveness gives us a foretaste of the possible effects of a politically motivated and targeted attack.

For an attack to be a genuine threat that could affect entire societies, either the target must be unique and indispensable or the attack must be one which, once triggered, uncontrollably cascades from one machine to the next. Last generation worms are examples of such 'cascade-caused failure' – they spread from one

47. A 'Boost sector' is the section on a disk (CD, HD or FDD) that contains information for the boot process of a device.

48. The 'Basic Input Output System' gives the computer the required information to access the Operation System (for example Windows or Unix). The BIOS is responsible for booting the computer by providing a basic set of instructions.

49. Raju Chebium, 'Love Bug virus raises specter of cyberterrorism', *CNN Interactive Correspondent*, 8 May 2000; http://archives.cnn.com/2000/LAW/05/08/love.bug/, viewed 29 November 2004.

50. These worms have their own SMTP engine, which is integrated in the source code.

computer to another very rapidly. To be so effective, they have to be specifically coded to exploit a weak spot of a targeted operating system.

In this context, IT *monoculture* acts as an important amplifier of attacks. The current market share of the most used web browser is almost 94 per cent,[51] and the market share of the most sold operation system is more than 97 per cent.[52] Such uniformity ensures perfect compatibility of systems and terminals, but it is also a perfect breeding ground for every computer virus. Moreover, the effectiveness of worms is enhanced if all computers use the same operating systems, and therefore have the same vulnerabilities.

Exploiting this monoculture, attackers of the most consummate skill batch together vulnerabilities to ensure failure by cascade. The NIMDA virus fully demonstrated that point – it used any of five separate application vulnerabilities to propagate itself.[53] In 2002, 70 per cent of all successful attacks exploited application vulnerabilities. Taking into account Slammer, Blaster and others that happened in 2003, the figure is now probably closer to 90 per cent.[54] Trying to close security gaps, software companies regularly come up with new 'patches' to be installed on computers. But up until now, virus programmers have always found an appropriate answer, and the time it takes them to develop a virus that exploits specific vulnerabilities is getting increasingly shorter. Given the inventiveness of virus programmers, the human nature of users and the existing monoculture, absolute security against viruses and worms will remain impossible.

Spillover effects on critical infrastructures

Modern societies increasingly depend on critical infrastructures in transport, energy and many other fields. These infrastructures are based on information systems that can become the victim of cyberattacks.

According to the European Commission, critical infrastructures 'consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic wellbeing of citizens or the effective functioning of governments in the member states.'[55] There is a broad spectrum of different critical infrastructures, ranging from oil and gas

51. Ben Hammersley, 'The second browser war', *The Guardian*, 15 July 2004; http://www.guardian.co.uk/online/story/0,3605,1260994,00.html, viewed 29 November 2004. However, other sources indicate lower market shares (w3schools estimates the market share of Internet Explorer at 74.1 per cent of all web browsers, and 89.7 per cent for Windows as the most sold operation system); http://www.w3schools.com/browsers/browsers_stats.asp, viewed 29 November 2004.

52. Ibid.

53. Dan Geer, Rebecca Bace et. al., 'Cyber*In*security: The Cost of Monopoly', 24 September 2003; http://www.ccianet.org/papers/cyberinsecurity.pdf, viewed 29 November 2004.

54. See Paul Desmond, 'All-out blitz against Web app attacks', *NetworkWorldFusion*, 17 May 2004; http://www.nwfusion.com/techinsider/2004/0517techinsidermain.html, viewed 29 November 2004.

55. Communication from the Commission to the Council and the European Parliament, 'Critical Infrastructure Protection in the fight against terrorism', COM(2004) 702 final, Brussels, 20 October 2004, p. 3.

distribution to electricity supply or air traffic control.[56] These infrastructures are both complex and increasingly interdependent; e.g. the disruption of one (for example electricity) will mostly have cascading effects and impact on others (such as air traffic). At the same time, many critical infrastructures today are (at least in part) privatised, which puts operators under constant pressure to reduce costs and ensure profitability.

In general, critical infrastructures are monitored and controlled by computer-based 'Industrial Control Systems' (ICS).[57] Automating industrial processes, these ICS typically collect sensor measurements and operational data, process and display this information, and relay control commands to local or remote equipment.[58]

One category of ICS — the so-called Distributed Control Systems (DCS) — evaluates data from process controllers in different machines of a plant and coordinates them. DCS can be used, for instance, to monitor the temperature of a series of reactors and at the same time control the rate at which reactants are mixed together.[59] DCS are typically used within a single processing or generating plant, or over a small geographical area. Another category of ICS is Supervisory Control and Data Acquisition (SCADA) systems, which are used for large, geographically dispersed operations,[60] such as water distribution systems, power lines, and oil or gas pipelines.[61] SCADA systems collect real-time data about processes or incidents and transfer it to a central site. More sophisticated SCADA systems can also determine the exact location, extent and nature of a possible incident.

Given the key role of ICS in the functioning of the overall system, they are prime targets for wrongdoers who want to disrupt critical infrastructures. However, in spite of their importance, they are often insufficiently protected against cyberattacks. For reasons of cost-reduction and efficiency, different ICS subsystems are increasingly connected with each other and, even worse, to other IT infrastructure. This is the case, in particular, for SCADA systems, because their data is transferred over long distances and – for reasons of economy – (too) often sent via data highways, which are also used by others for digital data traffic. Moreover, many operators have connected their ICS networks to their normal local area networks, which in turn are often connected to the Internet. 'Air gap' solutions, where computers connected to the ICS do not

56. Myriam Dunn and Isabelle Wigert, 'International CIIP Handbook 2004: Critical Information Infrastructure Protection', Andreas Wenger and Jan Metzger (eds.), CRN Publications, 15 February 2004; http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf, viewed 29 November 2004.

57. Dibya Sarkar, 'Protecting industrial controls', *Federal Computer Week*, 29 October 2004; http://fcw.com/fcw/articles/2004/1025/web-pcfrs-10-29-04.asp, viewed 29 November 2004.

58. Robert F. Dacey, 'Critical Infrastructure Protection: Challenges in Securing Control Systems', United States General Accounting Office, GAO-04-140T, 1 October 2003, p. 8; http://www.gao.gov/new.items/d04140t.pdf, viewed 29 November 2004.

59. Dana A. Shea, 'Critical Infrastructure: Control Systems and the Terrorist Threat', Report for Congress, 21 February 2003, p. 2.

60. Mark Longsdon, 'Threats and Vulnerabilities: What NISCC is seeing and how it is meeting the challenges', for the Critical Infrastructure Protection and Civil Emergency Planning, NIISC UK, p. 10; http://www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec/follow_up.p.html, viewed 29 November 2004.

61. See Gustav Lindstrom, 'Protecting European Homeland, Critical Infrastructures', *Chaillot Paper* (forthcoming).

have any physical connection to the outside world, are often considered to be too expensive.

Many critical information systems are thus within range of electronic attacks. The operators of critical infrastructures protect, of course, their LANs with firewalls, but if a wrongdoer succeeds in penetrating this line of defence, he will often have a walkover. At the time that ICS were initially being developed, they were either limited to a specific plant without any connection to the outside world (DCS), or were only accessible through dial-up modems (SCADA). Information security was therefore less important, and ICS were often designed without encryption technology or authentication processes. In consequence, data was – and still is – often sent as clear text, i.e. unencrypted; and protocols for accepting commands are not protected.[62] This modus operandi is not easy to reverse, because the hardware used for ICS is normally exactly dimensioned to fulfil the basic purpose of the system and does not have the necessary resources for additional functionality. Adding security tools for encryption and authentication now would thus also imply major investments in hardware, which many operators quite naturally try to avoid.

Moreover, operators increasingly use Windows or Unix as the basis for the operating system of their ICS rather than developing their own specific ones independently. Again, cost reduction is an argument here that plays into the hands of wrongdoers, who do not need to bother about the specificities of unknown operating systems, but can target commonly known vulnerabilities and make use of easily available and effective hacker tools (see IT monoculture above).[63] As a consequence, ICS become vulnerable to even non-targeted attacks. In January 2003, for example, Slammer – a worm programmed for the Windows operating system – hit the Davis-Besse nuclear power plant in Ohio. Despite the plant's protective firewall, the virus entered the safety monitoring system and disabled it for nearly five hours.[64] Since the plant was offline no further damage was done, but the incident gives an idea of the possible level of vulnerability of Industrial Control Systems.

Opinions about the actual threat of a cyberterrorist attack on ICS and its impact on critical infrastructures vary, and, in particular, the operators themselves tend to downplay the risks.[65] However, as for all other cyberattacks, it would be dangerous to assume that the threat does not exist merely because we have not yet

62. Dan Verton, 'Industrial control systems seen as "undeniably vulnerable"', *Computerworld*, 31 March 2004; http://www.computerworld.com/securitytopics/security/story/0,10801,91790,00.html, viewed 29 November 2004.

63. Dacey, op. cit. in note 58, p. 11.

64. See Kevin Poulsen, 'Slammer worm crashed Ohio nuke plant network', *Security Focus News*, 19 August 2003; http://www.securityfocus.com/news/6767, viewed 29 November 2004.

65. Ibid.

witnessed a major attack. At least the interest clearly exists. When authorities analysed seized computers of al-Qaeda activists, for example, they found out that research into the technical details on ICS of electricity grids, water systems and communication networks had been carried out.[66] Particularly worrying is the fact that the information used by the terrorist group was openly accessible on the Internet. And this was no exception: using open Internet sources only, a student at George Mason University succeeded in mapping all fibre optic connections leading to critical infrastructures in the United States.[67]

Fortunately, he did this only for his dissertation to prove that security measures were insufficient. However, it is yet another example of how careless use of the Internet can provide those of malicious intent with the perfect toolkit for an attack.

Conclusion

This chapter has illustrated how wrongdoers can use the Internet with malicious intent. The focus has been on politically motivated attacks, although the distinction between criminal and political misuse is often blurred. Terrorists, for example, can commit Internet fraud and use e-banking for money laundering, whereas criminal organisations may try to spy on confidential information, and they all use the same technical toolbox to pursue their objectives.

The security of information and information networks (Infosec) is a multifaceted challenge that can only be tackled using a comprehensive approach. There are, of course, technical solutions to protect our systems, and one can assume that in general the most attractive targets of cyberattacks will also be those that are best protected. However, the examples presented in this chapter show that an increasingly interconnected world will always contain security gaps. Moreover, many technical issues are closely related to market issues, and the existing monopolies of non-European companies are probably impossible to challenge. However, the alternative of open source software exists. It is rightly criticised for not being sufficiently user-friendly, but it is often cost-free and can reduce the vulnerability of systems. Public services in particular should therefore seriously consider this option in order to reduce costs and, even more important, to get a better insight into the system they use.

66. Sean Webby, 'Four Bay Area cities sanitized Web sites', *Mercury News*, 27 July 2002; http://www.mercurynews.com/mld/mercurynews/3560620.htm?1c.

67. Dacey, op. cit. in note 58, p. 13.

Equally important is encryption. One can assume – or hope – that public services dealing with classified information do not use the Internet to exchange such information, or at least use the tools of cryptology to protect it against spying. However, there is an important grey zone where information may be interesting for wrongdoers, even if it is not officially classified. Electronic mailing should therefore systematically be encrypted if the information is for the eyes of the receiver only.

However, in cyberspace even the most sophisticated technology will not be able to provide absolute security. Being connected to the Internet inevitably implies risks, even if protective measures are taken. At the same time, we should not forget that the advantages of the Internet far outweigh its dangers. The answer may therefore be not to reverse the trend towards greater connectivity but to manage its risks as effectively as possible.

In this context, it is important to remember that the main weakness of the system is often its user. Wrongdoers can regularly count on human behaviour to achieve their objectives. It is human curiosity that makes us open undesired e-mails and click on unknown hyperlinks, and carelessness that makes us send sensitive information unencrypted. The best way to deal with this human factor is to increase awareness of the risks. If users are aware of the risks they run when they go online, they may think twice before they click on the mouse. Awareness is thus an integral part of Infosec policy and should be given (at least) the same priority as technical countermeasures.

Besides human factors and technical challenges, Infosec also faces political and structural difficulties. Cyberspace is by its very nature anarchic, and Internet governance exists at best for technical aspects. The 'only globally visible body charged with any kind of oversight for the Internet' is ICANN,[68] but neither ICANN nor any of the other organisations which play a role in the technical coordination of the Internet deals with the misuse of cyberspace for criminal or political purposes.[69] In other words, there is no international authority responsible for issues concerning financial transactions, Internet content control, spam (unsolicited commercial electronic mail) or data protection and privacy.

In theory, a global tool like the Internet needs a global system of common norms, laws and law enforcement to fight its misuse effectively and proactively. Since such a system is not even a theoretical option, responses to offensive and criminal use of the

68. Cerf, op. cit. in note 11.

69. Besides ICANN, several private-sector-led organisations play a central role in the technical coordination of the Internet. The Internet Architecture Board (IAB) is responsible for the strategic technical direction of the Internet, including architectural oversight of Internet protocol and procedures, and standards development oversight; the Internet Engineering Steering Group (IESG) manages the Internet Engineering Task Force's (IETF) activities and Internet standards process; the IETF in turn is the principal body that develops Internet standards specifications; and, last but not least, the World Wide Web Consortium (W3C) develops interoperable specifications, guidelines, software and tools to promote the evolution of WWW, including html, portable network graphics and web accessibility guidelines. See *ICC Issue Paper on Internet Governance*, (Paris: International Chamber of Commerce, January 2004); http://www.iccwbo.org/home/e_business/policy/ICC%20issues%20paper%20on%20Internet%20Governance.pdf, viewed 29 November 2004.

Internet inevitably face a structural handicap. Whereas wrongdoers can fully exploit the global and unregulated nature of the Internet, the fight against them is often fragmented at the national level or, at best, loosely coordinated in intergovernmental frameworks.

This puts limits on European cooperation in this field as well. Granted, Information Society and Technology have been on the agenda of various EU forums for some time, and cooperation in related areas such as Justice and Home Affairs and Research contribute to enhance IT Security. However, Infosec is a vast field with plenty of different stakeholders. In particular those areas where state bodies and 'traditional' security institutions are concerned, cooperation, if it exists, is still organised in a purely intergovernmental way, which stands in stark contrast to the nature of cyberspace and its related threats and risks. The following chapter will describe how the EU and its individual member states try to cope with these dilemmas.

National and European information security policies

Alain Esterle

2

The bases of Infosec policies in Europe

In Europe, the purpose of security policies on information (the contents) and information systems (the container) is to protect the information (integrity), to guarantee its terms of access (availability, confidentiality, identification of correspondents) and its evidential value (authentication, non-reputability). These properties are essential in order to guarantee the independent execution of state policies, as well as the reliable use of IT in important socio-economic areas (online exchanges for administrations, trade, education, health, etc.).

Three types of actors are affected by these applications and by Information security – currently dubbed 'Infosec' – that underpins them:

- *the citizen*, particularly concerned with personal data protection, an essential condition of individual freedoms in democratic states, and, as a consumer, with the quality of the services he/she is buying;
- *companies* whose operation and success, if not their very survival, are closely related to the protection of their know-how, the respect of intellectual property rights, fair competition, and the trusted functioning of production and distribution processes that are dependent on increasingly complex information systems;
- *the state apparatus* responsible for protecting sensitive and, a fortiori, classified information and for the security and operational continuity of institutions and infrastructures that are vital for socio-economic activities.

In each of these areas the aim is to secure the information and associated systems or networks through a number of technical, operational and legal conditions that must take into consideration both the need to preserve individual freedoms and the

potential development of criminal practices. In other words, Infosec policy is always a compromise between the preservation of individual freedoms, the implementation of restrictive security regulations and allocations of material and human resources.

Infosec policy finds its expression in technical or operational procedures and legal regulations. In line with the general guidelines adopted by the OECD (see Annex 2),[1] these regulations and procedures may be broken down into three complementary areas:

- *risk management:* which includes threat analysis; a clear identification of security needs in terms of confidentiality, integrity and/or availability of the information to be processed; assessment of the legal environment and operational constraints; and the sharing of responsibility between the different actors. This issue is closely related to awareness raising, risk assessment methodology and best practices;
- *secure equipment and services:* in order to attain the security objectives specific to a given information network, secure equipment and services must be implemented with technical, operational and human characteristics. This needs equipment evaluation capabilities, Infosec training and the licensing of high-quality service providers;
- *response to cyberattacks:* this consists of setting up teams specialised in forewarnings, alerts and responses to all types of incidents affecting information networks. It also includes building a legal apparatus that can clarify the criminal nature of certain acts and the services empowered to start legal proceedings.

As in many other fields, the European authorities assume general responsibility for harmonisation and guidance, for raising awareness and the establishment of a coherent legal apparatus through the adoption of directives and framework decisions.

As for authorities at the national level, they have to adapt their national law to European directives. It is their job to implement the operational and practical framework and to ensure that it functions properly and in accordance with the guidance agreed under the Union's second and third pillars, particularly protecting against, responding to and sanctioning of criminal acts.

We must next examine how different or how close the national policies are at the moment, and how actions at the national and European levels complement each other. From this, it will be possible to identify weak points and focus on priorities for future initiatives.

1. Recommendation of the Council of the OECD: 'OECD guidelines governing the security of information systems and networks – Towards a culture of security', 1037th session, 25 July 2002.

National Infosec policies: a common heritage

At state/national authority level, Infosec looks as if it has been inherited from the time when cryptography was a weapon that states had to control, in order to protect their most secret military or diplomatic information, and at the same time try to retrieve information that hostile states were themselves trying to protect. Thus, defensive and offensive approaches have been closely interlinked.

Towards the end of the 1990s, the widespread use of information and communication technologies for paperless exchanges between citizens, businesses and administrations became a general trend in European countries, which were all facing the same need to increase productivity and growth in order to cope with the demographic changes taking place in their society. However, this also meant that all these different users had to have complete confidence in the security of the systems, and that this had to be based on the same methods, techniques and practices used for the security of state information. It was no longer possible to reserve these security tools for state duties alone. Consequently, the conditions for delivering and using resources in cryptography, for example, were made easier and common evaluation and certification standards for security products were adopted to promote the development of an open market for these products (see below).

Rather than go into details of the legal, organisational and technical framework in each European country, it seems more fruitful to identify their common features and their differences, and to illustrate these by comparing a few countries who are particularly active in the field.

Institutional Infosec disparities

Generally speaking:

- ministries are responsible for the security of their information and information systems;
- a national agency[2] is responsible for setting national policy. It has a number of national prerogatives (cryptography assessment, manufacture of keys, etc.) and provides a number of services to all ministries. It acts as the recognised negotiator in respect of international relations (particularly a NATO requirement).

2. Sweden, a major country in the field, does not yet have one but has instigated a wide-ranging process of reflection due to end in 2004-05.

Often at times this agency is, as in the United States, assimilated into the signals intelligence (SIGINT) services (as in the Netherlands, Spain and the United Kingdom). This choice indicates whether priority is given to cohesion between the defensive and offensive aspects of Infosec in response to government requirements or to the more general security needs created by the growth of the information society. This choice also has an effect on the image of the agency and the audience it is able to serve at the national and international level.

Furthermore, this agency may report directly to the Head of Government (as in France and Spain) or be part of a particular ministry (Germany, United Kingdom). More often than not, it maintains very close relations with the government authority responsible for the development of e-Government (eGovernment in the United Kingdom, ADAE in France).

For the past two or three years, these national agencies have seen their resources increase significantly because of both a new threat perception in the aftermath of the terrorist attacks of 11 September 2001 and the increased need for security in new sectors (health, online government, etc.).

Institutional organisation of Infosec agencies

Country	Name	Approximate workforce	Ministry attached to	Integrated into SIGINT body
Germany	BSI[3]	425	Interior	No
France	SGDN/DCSSI[4]	100	Prime Minister	No
Spain	CNI/CCN[5]	40	President of Government	CNI
Netherlands	GISS/NLNCSA[6]	40	Interior	GISS
United Kingdom	GCHQ/CESG[7]	450	Foreign Affairs	GCHQ

The human resources in these agencies are not correlated with conventional socio-economic parameters such as population or GDP, but rather with the range of activities. For example the French DCSSI does not work directly on the development of equipment, CNI/CCN is not involved in civil applications, etc. In the United States, the duties of this agency are performed by the Information Assurance Division (which has a full range of

3. Bundesamt für Sicherheit in der Informationstechnik.

4. Secrétariat général de la défense nationale / Direction de la sécurité des systèmes d'information.

5. Centro Nacional de Intelligencia/Centro de Criptologia Nacional.

6. General Intelligence and Security Service/NederLand National Communication Security Agency.

7. Government Communications Headquarters/Communications Electronics Security Group.

activities) of the National Security Agency (an estimated 2,900 persons). Even if we were to put all the European resources together, which would not currently make a great deal of sense, they would still fall short of those being mobilised in the United States.

Security product development and evaluation capability: a shared need at the national level

The market for commercial products that contribute to Infosec is largely dominated by a small number of non-European manufacturers. Despite the development of open sources software, this quasi-monopolistic situation on significant segments of the market (e.g. operating system for work stations) may have a very negative impact in terms of security.

In several European countries, a number of evaluation procedures have been set up in order to give the consumer (citizen, enterprise, administration) some security guaranty. These evaluation procedures consist of verifying that the products are actually doing what they are supposed to do, and whether they are resistant to different kinds of attacks.

Generally speaking, the evaluation procedures conclude with a certificate by which the national Infosec agency guarantees that the evaluation has been correctly performed. On the other hand, national agencies do not necessarily carry out the assessments themselves.

- All national agencies evaluate *cryptographic algorithms* internally. Nearly all of them evaluate *cryptographic products* (algorithm implementation) internally. Only France and Spain rely for this purpose on a Ministry of Defence laboratory. In Spain, the National Cryptology Centre (CCN) is trying to assimilate this activity within its own administration.
- Electronic equipment that is currently used emits electromagnetic waves that can be intercepted and, under certain conditions, analysed to restore the original information. Technical tests can be performed in order to check for such *compromising emissions* (TEMPEST[8]). In this field, the trend is to outsource this evaluation activity.[9] The evaluation can be subcontracted or carried out at the premises of the manufacturers under state control. Only organisations with substantial resources (BSI) still carry out TEMPEST evaluations internally.

8. Test for Electromagnetic Propagation and Evaluation for Secure Transmissions. Other current spelling: Transient ElectroMagnetic PulsE STandard.

9. The first agency to do so was the CESG, which had as many as 50 people engaged in this activity, but now has fewer than 10, and relies on industrial resources (or on the Ministry of Defence) to carry out these assessments.

- Besides cryptographic tools and compromising signals, general *IT security product evaluation*, which is quite recent, has from the beginning been carried out by private laboratories approved by the national Infosec agencies on the basis of public standards. A major drive was instituted in the 1980s to establish an internationally recognised standard called the Common Criteria for IT Security Evaluation, which became ISO standard 15408. It is widely used today for the assessment of non-cryptographic security products. More recently, the American NIST[10] set a standard for cryptographic modules, the FIPS140-2. In the general interest of controlling public expenditure, the current trend is to use the standards of the Common Criteria for evaluation and certification, and FIPS140-2 for the assessment of cryptographic products. Only cryptographic algorithms and very high-level security products are still evaluated by national Infosec agencies. The private laboratories that evaluate Infosec products are controlled by a certification centre which issues the final certificate (in the framework of a national evaluation/certification scheme). In all major countries, the certification centre is part of the national Infosec agency, as is the case in the United States, even if private certification bodies exist at the same time.
- A *mutual recognition agreement* signed in 1999 by EU member states validates the evaluations/certifications carried out in any of the signatories operating a recognised national evaluation/certification scheme. At a more international level, in May 2000, the Common Criteria Mutual Recognition Arrangement (CC-MRA) was established to recognise Common Criteria certificates (but only up to level EAL 4[11]) between the parties. These agreements introduce more flexibility into the security equipment market of countries that specialise in such technology.

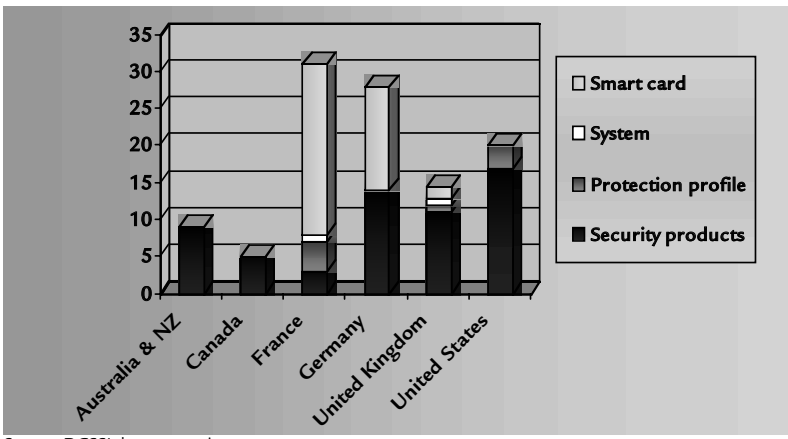
However, even though these evaluation procedures may give a good guaranty that the equipment is actually doing what it is supposed to do, it cannot guarantee that it will not potentially affect – wittingly or not – the confidentiality, the integrity or the availability of the information being processed. No technical test, including source code analysis,[12] is currently able to provide this type of guaranty, which requires close and trusted relations with industrial partners at all stages of the product's development. Thus, a

10. National Institute for Standards.

11. EAL is the evaluation assurance level, i.e. the depth of the assessment performed to verify that the functionalities included in the 'target of evaluation' are operating correctly. The developer has to provide evidence that his source code meets the 'target of security', and the quality of evidence determines the level of evaluation to be reached, from EAL 1 to EAL 7. For EAL 5 and above, formal mathematical models are used, leading eventually to formal proof of security. However, such mathematical models can only be used if they have been introduced into the software design and development process. This is not the case for commercial products, where there is no call for such high levels of evaluation.

12. Contrary to a very common belief, there exists no formal or practical method yet to analyse exhaustively the hundreds of thousands or millions of instruction lines of today's software programs if they have not been designed and developed in an appropriate way (using formal mathematical models of proof). For complex software, even the use of such models cannot guarantee the non-existence of a hidden property. Therefore, a trustful relationship with the developer is crucial.

Number of certificates delivered in 2003,
per technology and national scheme



Source: DCSSI documentation

number of governments are exercising direct control over the development of the products they use to protect their classified information (for which the mutual recognition agreements do not apply). Along this line, high-level security cryptographic products always emerge from government developments. Following the example of the United States, it is generally the national Infosec agency that is responsible for these developments (Germany, Netherlands, Spain, the United Kingdom). In France this activity is currently in the hands of the defence procurement agency (DGA) at the Ministry of Defence.

The funding process varies according to the organisations. In Germany, for example, the budget of the BSI includes the cost of product development, whereas in the United Kingdom and in the Netherlands the ministries have to fund the development of the products they need. The problem with this approach is that ministries may fail to express any need for products because they do not wish to assume the development costs on their budget, preferring to wait for another Ministry to do it instead.

To overcome this difficulty, it has been agreed in the United Kingdom that the eGovernment office, which manages the development of electronic administration, will take over responsibility for interdepartmental needs. Its task is to get the CESG to develop security products that are of interest to more than one ministry. In the Netherlands, the decision has recently been taken to set up an entity dedicated to developing security products. The main ministries involved make a contribution to its budget in the form of a

one-off sum fixed at the start of the year, which makes the expression of needs much easier for the Ministries. This agency is now operational and has been incorporated into the national Infosec agency (NLNCSA).

Information security services: a market aiming for self-regulation

Infosec services have grown widely in recent years. In addition to conventional cryptographic key management, security consulting and advisory services, intrusion detection services, operating network security, certifying the root keys of the Public Key Infrastructures (PKI), etc. have been added.

Carrying out these activities, which are crucial for security, requires confidence in the organisation involved. This can be obtained either by having these services provided within the administration (typically by the national Infosec agency), or by controlling the activities of private service providers or by developing trust labels which the latter are encouraged to obtain.

Cryptographic key management is still traditionally one of the most highly regulated activities, which is why the CESG (for the United Kingdom), the NSA (for the US DoD), DACAN (for NATO) and the NLNCSA (for the Netherlands) still have a monopoly over the manufacturing of keying material for their government. None the less, since this centralisation is very cumbersome, the trend towards decentralisation is becoming increasingly marked, with governments in most cases retaining some control (declarative system, mandatory handover of keys, etc.).

At the same time, national Infosec agencies provide their administration with a more or less extensive range of services, namely consulting, monitoring of protected communications, intrusion detection control, etc. Sometimes the agencies are paid for these services (CESG).[13] They offer services in technical fields where they have considerable expertise, but do not aim to cover all possible activities. So far none is developing services devoted to network security monitoring. Additionally, a number of new services may also be provided by other administrations (particularly for governmental PKI certification).

In general, a large share of the security service market is covered by private service providers who have developed in response to the various needs of the private and public sectors. The current trend

13. Including manpower support to industrial product development, according to CAPS (CESG Assisted Product Scheme).

is not towards strict control of their activities, but rather towards licensing these service providers. Britain's CESG was the first to go down this road, with among others the CLASS programmes for licensing consultants and the IT-Health Check programme for carrying out technical IT audits. In the same way the BSI has recently set up an auditor accreditation programme complying with its IT audit standard (IT baseline protection manual). As part of its strategy to make cyberspace secure, the US administration is also indicating that it will look into setting up licensing programmes of this kind. In France, the state's objectives of its IT security reinforcement plan include mechanisms for licensing private service providers. In 2005, a qualification scheme is expected to be introduced that guarantees conformity of certification service providers and time-stamping service[14] providers to a 'security reference policy' set of rules.

This trend towards licensing is widespread, because professions are feeling the need to promote the standardisation of business plans and the development of fair competition. Today the international standard ISO17799 is becoming increasingly accepted as the general criterion for IT security certification.

It should be noted that the vigour with which the national Infosec agencies are promoting the transfer of business to the private sector is in line with national choices in the field of economic and administrative organisation, even if the activities considered to be the most critical are still performed by the public authority.

Response to attack and critical infrastructure protection: national public and private approaches that need better coordination

Since the end of the 1990s, EU member states have developed operating and legal structures to provide an effective response to attacks on networks and to give better protection to critical national infrastructures. These bodies fall into three main categories:

- CERT[15] or CSIRT[16] are public or private technical teams that watch, warn and respond to attacks;
- Computer Crime Units (CCUs) are responsible for prosecuting crimes related to the use of information and communication technologies;
- other bodies dedicated to the protection of critical infrastruc-

14. Time stamping makes it possible to prove that some unambiguous representation of data exists before a given time.

15. Computer Emergency Response Team (terminology introduced by the Carnegie-Melon Institute).

16. Computer Security Incident Response Team (European abbreviation).

tures and vigilance and intervention plans to deal with high-intensity attacks on networks.

The EuroCERT project (1999-2000) was an attempt at centralising the coordination of monitoring and warning activities, but the economic model turned out to be inadequate and it was therefore abandoned. Since then, the number of specialised teams with academic, governmental or commercial status has gradually increased among most of the member states. By October 2004, 89 CSIRTs were spread over 30 countries in and around Europe, and 41 of them are accredited by the TF-CSIRT,[17] which is a coordinating body that launches initiatives in training, standardising (categorising incidents) and setting up secure links where appropriate. Particular stress is placed on the availability of monitoring and warning resources for small and medium-sized enterprises (SME).

Many member states have governmental CERTs specially dedicated to responding to attacks on the state's information systems. They have regular meetings on the fringe of the TF-CSIRT.

It may be noted that the total number of CERTs in a given country, including the CERTs dedicated to businesses, has apparently less to do with the size of the country than with the expected level of independence of the private sector, the freer the market, the greater the number of private CERTs.

Number of CERTs or CSIRTs accredited by TF-CSIRT, amongst those listed (in brackets)

Austria	**1** (1)	Greece	**1** (2)	Slovenia	**1** (1)
Cyprus	(1)	Hungary	(2)	Slovakia	
Czech Republic	(1)	Ireland	(1)	Spain	**2** (3)
Belgium	**1** (1)	Italy	**1** (2)	Sweden	**2** (3)
Denmark	**3** (3)	Latvia		The Netherlands	**4** (9)
Estonia		Lithuania	(1)	United Kingdom	**4** (13)
Finland	**2** (2)	Malta	**1** (1)	Trans-European	**2** (4)
France	**2** (4)	Poland	**1** (3)		
Germany	**8** (15)	Portugal	**1** (1)		

Source: TF-CSIRT as of October 2004

Most member states have also set up units dedicated to investigating computer-related crime, so called Computer Crime Units (CCUs).[18]

17. The TF-CSIRT Task Force is established under the auspices of the TERENA (Trans-European Research and Education Network Association) to promote collaboration between CSIRTs in Europe.

18. See 'Computer related crime within the European Union', file number 2560-43-Rev2, Europol.

The task of CCUs is to instigate legal proceedings subsequent to attacks on networks. In this, they are able to rely on the support of the CERTs or CSIRTs, which provide them with technical expertise. But their work may also focus on conventional crimes that make use of information systems, and in that case the CCUs provide back-up for conventional investigation services, for example in helping to identify certain perpetrators of criminal acts.

Most of these teams are small-scale in relation to the size of the task, and a good part of their activity consists in coordinating the actions of other investigation teams. Few of them carry out systematic network surveillance. In the United Kingdom, the national organisation known as the NHTCU[19] provides coordination with local correspondents throughout the country, cooperation between agencies and links with industry. In France in May 2000, the OCLCTIC[20] was set up in the Ministry of the Interior to conduct legal enquiries of a highly technical nature and to train investigators specialising in computer crime in the regional branches of the Criminal Investigation Department. At the same time, OCLCTIC acts as the National Contact Point for international authorities (Europol, Interpol, G-8).

In general, these CCUs require internal growth, coordination with the other national services responsible for Infosec, and operational cooperation with their counterparts in other countries (cross-border investigation).

Member states also face the danger that major attacks on networks may paralyse or cause lasting damage to a number of the infrastructures that are essential to the continuance of socio-economic activity in the country: telecommunications, transport, power supply, health, banking system, etc. Following the example of the United States, governments in Europe have launched specific actions for the protection of these critical infrastructures and related information networks.[21]

Thus in the United Kingdom, the NISCC,[22] attached to the Home Office, relies on the support of the UNIRAS (governmental CERT) to provide operators of critical infrastructures with technical advice, information about threats, vulnerabilities and warning levels. It also relies on the support of the WARP,[23] which is responsible for recording warnings and reporting incidents (but with no intervention capability) and the ISAC,[24] which disseminates information about warnings and incidents within a given community of users, generally on a commercial basis.

19. National High Technology Crime Unit.

20. Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.

21. Concerning critical information infrastructures, a distinction is usually made between digital control systems (DCS) and supervisory control and data acquisition systems (SCADA).

22. National Infrastructure Security Coordination Centre.

23. Warning, Advice and Reporting Point.

24. Information Sharing and Analysis Centre.

In Germany, the protection of critical infrastructures is entrusted to the BSI, which carries out exercises involving administrations (ministries of the interior, defence, transport, telecommunications) and industries (EADS).

In France, this task is entrusted to the Secrétariat général de la Défense nationale (SGDN), to which the national Infosec agency (DCSSI) is also attached. Protection is provided both by regular inspections at a series of sensitive points and networks in all parts of the country, and by vigilance and intervention plans. These plans actually take into account the threats to information networks, and regular exercises involving all or part of the state apparatus and critical infrastructures test response capabilities.

These national developments have not yet resulted in any genuine operational coordination, for example joint exercises, or joint warning activations, and it is proving difficult to properly set up collaborative activities (e.g. networks of correspondents 24 hours a day, 7 days a week) advocated in the Council of Europe's convention on cybercrime[25] and in the G-8 principles on the protection of critical information infrastructure (see Annex 3).[26] Moreover, vigilance and intervention plans, when they do exist, are specified and organised on a national level, whereas threats and attacks are cross-border in nature. The final paradox is that the protection of critical infrastructures is designed and organised at a national level, whereas the operators of these infrastructures see their activity and their organisation on a European or even wider level, where deregulation is a prerequisite.

An overall convergence of national policies, but deep disparities nevertheless

Infosec activities in member states have evolved in a similar way, and there is an increasing convergence between the various Infosec policies. This is based on common adherence to the EU's Charter of Fundamental Rights, democratic principles, respect for individual rights and a market economy. The participation of most member states in a common defence organisation (NATO) that specifies methods is also fostering similarities. This convergence has found its expression in the adoption of the OECD guidelines governing the security of information systems and networks ('Towards a Culture of Security'),[27] the signing of the Council of Europe Convention on Cybercrime and, more recently, the adoption of the G-8

25. *European Treaty Series*, no. 185; 'Convention cybercrime', Budapest, 23 November 2001. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. The Convention is the product of four years' work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the organisation. It will be supplemented by an Additional Protocol making the publication of racist and xenophobic propaganda via computer networks a criminal offence.

26. Principles adopted by the Ministers of Justice and the Interior of the G-8 countries on 5 May 2003. They have been integrated in Resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, adopted by the General Assembly of the United Nations on 30 January 2004.

27. Recommendation of the Council of the OECD: 'OECD guidelines governing the security of information systems and networks – Towards a culture of security', 1037th session, 25 July 2002.

principles for the protection of critical information infrastructures.[28] On top of this comes an intergovernmental mutual recognition agreement covering the full range of evaluation/certification levels for security products that aims at promoting the development of a competitive market within the Union. Last but not least, the Council has adopted a great number of directives; once incorporated into national law, they form an increasingly homogeneous legal framework for the protection of privacy in the electronic communications sector, evidential value of electronic signature, etc.

However, in spite of wide similarities and undeniable convergence, powerful national prerogatives and important disparities persist that should not be underestimated. The delivery and use of cryptography have been deregulated, but specialist skills in assessing algorithms and designing high-tech equipment still remain mainly in the hands of government authorities. Moreover, these skills are still fragmented at the national level: there is no significant transfer of know-how between governments, and exchanges are made on a reciprocal basis, which does not help reduce disparities.

It should also be noted that, so far, cooperation in the development of government security products is rare. Moreover, there is a lack of coordination in attempts to preserve diversity in the supply of security products, in terms of both relationships with suppliers who are in a position of quasi-monopoly and support for the development of open-source software.

Finally, there still remains a division between the 'well-equipped' countries, which have for a long time invested in cryptography in support of state secret and intelligence information, and those that have (willingly or not) neglected this domain. The former have been able, each one in their own way, to adapt their scientific, technical and operational capacity to the new context, while the latter have encountered difficulties in being acknowledged as valuable partners.

But other dividing lines exist within the member states, even those with the most advanced Infosec capabilities. For instance, a fracture between political will and day-to-day practice, or between Infosec awareness of state bodies and that of the citizen, or between major enterprises able to set up and finance a fully-fledged Infosec policy and SME. Yet the Infosec issue does not only depend on governments and their (more or less dynamic) policy,

28. Principles adopted by the Ministers of 'Justice and Internal Affairs' of the G-8 countries on 5 May 2003. They have been adopted by the General Assembly of the United Nations – Resolution 58/199 of 30 January 2004 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures.

but concerns all actors in the information society, from the private and the public sectors to the citizen as well as associations, since the level of security of increasingly interconnected systems is still that of its least secure element.

And here the European Union certainly has an important role to play.

The EU's growing role in Infosec

Unlike the member states, the European institutions have no historical legacy in the protection of classified information or in intelligence activity.[29] Current EU policies in the field of Infosec have been inherited from economic and monetary policy, not from the (more recent) European security and defence policy (ESDP).

Although there are some limited activities that precede it, the founding element may be considered to be the 'Lisbon strategy', which was adopted by the Council in March 2000.[30] The widespread and reliable use of information and communication technologies for all social categories was presented therein, and confirmed four years later,[31] as a basic tool for making the EU '*the most competitive and dynamic knowledge-based economy in the world*'.

To this end, the Commission has called on its traditional tools: action plans, directives and R&D programmes. But the pressure of the international situation is gradually causing the Union to extend its field of operations to take into account ESDP issues. The creation, in 2004, of a European agency specifically dedicated to the security of information and networks represents a major step forward.

Developing the Union into an information and knowledge society

To implement the Lisbon strategy, an action plan called 'eEurope – one information society for all' was instigated. In the first stage, from 2000 to 2002, it sought to:

- give access to a less expensive, faster and safer Internet;
- invest in people and skills;
- stimulate Internet use.

29. WEU Assembly Recommendation 707, 'On the new challenges facing European Intelligence', Explanatory Memorandum, Mr Lemoine, Rapporteur, 2002.

30. Before 2000, the European Commission had set up a Senior Officer Group for information society (SOG-IS) whose recommendations led to the adoption in 1997 of a Mutual Recognition Agreement for using the ITSEC criteria to evaluate security technology, and to its extension to common criteria in 1999. It is worth noting also the electronic signature directive in December 1999.

31. 'Challenge for the European Information Society beyond 2005', Commission Communication COM(2004), 757 final, Brussels, 19 November 2004.

At the end of this first stage, the measuring instruments set up by the Commission (benchmarking) showed[32] that the Internet penetration rate in private homes remained small, even if it had more than doubled over the period (from 18 to 38 per cent), which was still low relative to the penetration rate in businesses with more than 10 employees (90 per cent connected to the Internet, 60 per cent with their own website). Above all, these measurements highlighted a great disparity between the different member states.

The report also recorded an increase in the number of threats and a worrying slowness in installing security products in networks and workstations. Despite the adoption of the 1999 directive,[33] the electronic signature market was still in its infancy, and the major smart-card industrial project, supported by a research grant of €100 million, had not yet produced much in the way of results.

Consequently, the second stage of the eEurope Action Plan, from 2002 to 2005,[34] is directed towards '*the widespread availability and use throughout the European Union by 2005 of broadband networks, the development of Internet protocol IPv6 . . . and the security of networks and information, eGovernment, eLearning, and eBusiness*'.

In the field of security, the action plan stresses the development of a security culture, support for warning networks, research under the 6th Framework Programme (FP6) on confidence-building, certain technologies (broadband, wireless links, intelligent environment, etc.) and the needs for high-security networks to protect certain information, whether it is commercial or not. It also underlines the need for the creation of a European entity dedicated to network and Infosec.

The mid-term report has recently acknowledged the difficulty in demonstrating that progress in bringing Europe online has actually resulted in new jobs and services or an increase in productivity as recorded elsewhere, particularly in the United States. The networks and the interconnections are in place, but they are not being used, in particular on account of a lack of confidence. Nearly 80 per cent of European citizens do not yet dare to make online purchases, because they are afraid of a lack of security, in a context where only 54 per cent of businesses have formally adopted a security policy.[35]

32. COM(2002), 62 final, 5 February 2002.

33. CE directive 1999/93, implemented 19 July 2001.

34. COM(2002), 263.

35. COM(2004), 108 final, 18 February 2004.

Developing a legal framework for strengthening trust

In the fight against computer-related crime, the Commission Communication of 26 January 2001[36] presents a survey of the European situation and offers some guidance.

A number of non-legislative measures are advocated therein, both at the national level (setting up of specialised CCU-teams), and also in terms of cooperation at the European level. In this way, several groups of the JHA Council have taken Infosec into account in their work: the 'Police cooperation' group; the multidisciplinary 'organised crime' group; and the 'Article 36' committee, which examines the work of all third-pillar groups. Finally, Europol monitors and reports, on a regular basis, on questions about computer-related crime at the European level. The communication also recommended that all member states join the network of points of contact competent in law enforcement, set up by the G-8 to operate 24 hours a day, 7 days a week in handling urgent requests for cooperation in the field of electronic evidence. Its operation continues none the less to be problematic, largely for manpower management reasons.

At the legislative level, the communication went back to the first principles already enshrined in European law, particularly with regard to the confidentiality of communications and the legal conditions for interception, traffic data retention, the lawfulness of the contents or intellectual property.

If the precise specifications on the legal conditions for intercepting communications have not led to an agreement between the member states, the directive 2002/58/CE of 12 July 2002[37] returns to the question of handling personal data and the protection of privacy. It sets out the rights of the individual, both as a consumer (it is up to the supplier of an electronic communication service to guarantee the security of his services), and as a private person (the member states guarantee the confidentiality of communications . . . and of traffic data).

This directive thus specifies that traffic data is to be deleted or depersonalised as soon as it is no longer needed to send or prepare invoices, but none the less leaves the state the possibility '*of adopting legislative measures providing for the retention of data for a limited period*', subject to these measures being '*appropriate or proportionate, within a democratic society, to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of*

36. 'Creating a safer information society by stepping up the security of the information infrastructures and combating computer related crime', COM(2000), 890 final.

37. Directive 2002/58/CE is part of the extension to Directive 95/46/CE relating to personal data protection and to Directive 97/66/CE on the handling of personal data in the telecommunications sector, the latter being on this occasion repealed.

criminal offences or of unauthorised uses of electronic communication system.' In the wake of 11 March 2004 in Madrid, the European Council adopted a declaration on combating terrorism, calling notably for the establishment of rules on traffic data retention.[38] A framework decision proposal prepared by four countries (France, Ireland, Sweden and the United Kingdom) was submitted to the Council in June 2004[39] and should be adopted before mid-2005.

Unwanted communications (or 'spam') and unlawful contents have, for their part, given rise since 1999 to a succession of multi-annual community programmes (Safer Internet programme) which have proven the resolve of the Council and the European Parliament on this subject. The most recent step is the Commission Communication of 12 March 2004 proposing to the Parliament and to the Council that, after the Safer Internet Action Plan (1998-2004), [40] they set up another programme to promote safer use of the Internet and new online technologies (Safer Internet Plus,[41] with a budget of €50 million over three years).

In relation to e-commerce, the directive 1999/93/CE on electronic signatures has been properly incorporated into the national legislation of member states, so far without producing the expected changes. The market in certification service providers is still small, particularly with respect to the delivery of qualified certificates, and e-commerce is not growing as fast as expected. None the less, no revision of this directive, which was originally envisaged, will be undertaken in light of results of a study conducted on this subject. Efforts will focus instead on the recognition of prescriptive implementation documents and on the security of essential functions (archiving, time stamping). The directive interpretation problems are discussed between national representatives in the framework of an informal forum called FESA.[42]

R&D and deployment programmes: supporting the Lisbon strategy and beyond

The Commission has also become increasingly active in the field of research on information and networks security.

Over the period 2002-06, the 6th Framework Programme is devoting €3.62 billion to information technologies,[43] of which €50 million are reserved for the theme 'Towards an overall frame-

38. Declaration on combating terrorism, CEU 7906/4, 29 March 2004.

39. Draft Framework decision on the retention of the data processed and stored in connection with the provision of publicly available electronic communication services or data on public communication network for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, no. 8958/04 Crimorg 36 Telecom 82 of 28 April 2004.

40. See Decision no. 276/1999/CE of the Parliament and the Council of 25 January 1999 (OJ L 33, 6.2.1999, p.1) to adopt a multi-annual community action plan for the purpose of promoting safer use of the Internet by combating messages with illegal and harmful content disseminated on the world networks, extended by Decision no. 1151/2003/CE of the European Parliament and Council of 16 June 2003 (OJ L 162, 1.7.2003, p. 1). See also the Decision of the Council of 29 May 2000 on the fight against child pornography.

41. The objectives being (a) fighting against illegal content, (b) tackling unwanted and harmful content, (c) promoting a safer environment and (d) awareness-raising.

42. Forum of European Supervisory Authorities for Electronic Signature, comprising 18 member states, 2 member states of the EEE and a candidate country.

43. The total budget of the FP6 amounts to €17.5 billion (including Euratom) over the period 2002-2006. In comparison, the FP5 had a budget of €15 billion from 1998 to 2002, including €3.6 million for the information society technologies.

work of confidence and security'. Although small, this amount makes it possible to establish links between different research teams in Europe, including two from the Joint Research Centre.[44]

In line with FP6, the eTEN (trans-European networks) programme is devoted to the achievement of the eEurope programme objectives, including those on security and dependability. Based on R&D results, it is aimed at the implementation and deployment of telecommunication networks based services (e-services) with a trans-European dimension. It promotes public interest services that give every citizen, enterprise and administration full opportunity to gain from the e-Society.

The directorate general 'Information society' (DG InfSo) is piloting the 'Information Society Technologies' (IST) programme, managing actions for the preparation (objectives) and follow-on (selection of proposals, evaluation) of the Framework Programme and eTEN. Recent discussions[45] tend to consider IT as heterogeneous technological infrastructures with a configuration that is variable in time and space (wired or wireless links, use of mobile telephones and computers, etc.). Applying a consistent security policy to this type of information infrastructure raises a new and widespread methodological problem, whether this infrastructure relates to a housing unit, a town, a country or Europe. These new paths will have to be taken into account in the preparation of the next Framework Programme (FP7).

A major change has taken place in the context of the terrorist attacks of 11 March 2004, with the decision to initiate a new research activity devoted to internal and external security.[46] On the basis of a report by a Group of Personalities (GoP),[47] the Commission has set up a Preparatory Action on Security Research with €65 million from 2004 to 2006) devoted to advanced technological industrial research in combating terrorism, preventing and responding to weapons of mass destruction[48] and protecting information networks, whether targeted against civilian populations or forces engaged in external operations. According to the Commission, this Preparatory Action should, by 2007, lead to a full-fledged European Security Research Programme (ESRP). Based on a comprehensive security approach, an ESRP goes far beyond (or beside) the Lisbon strategy and may be considered as an acknowledgement of the legitimacy of the EU's role in Infosec.

44. One team at the Institute for long-term technical and scientific planning (IPTS) in Seville on the social and legal aspects of IT development, and the other at the Institute for the protection and security of the citizen at Ispra (Italy), for the validation of security equipment on the basis of skills acquired during nuclear safety operations.

45. Workshop on 'R&D challenges for Resilience in Ambient Intelligence', 19 March 2004.

46. COM (2004), 72 final, and Decision 2004/213/CE, 3 February 2004.

47. *Research for a Secure Europe*, Office for Official Publications of the European Communities, Luxembourg, 2004; http://www.iss-eu.org/activ/content/gop.pdf.

48. Nuclear, radiological, bacteriological and chemical (NRBC). See 'Protecting the European homeland – the CBR dimension', *Chaillot Paper* 69 (Paris: EU Institute for Security Studies, July 2004), p. 48.

Putting EU policy into practice

Alongside the legislative, programmatic and promoting EU actions l, at least three action lines may be noted which have led the Union to assume growing operational responsibilities in Infosec.

Communications between national and EU administrations

Since 1999, the European Commission has undertaken to develop communications between the administrations of the member states and the Union.[49] At the end of 2003, this programme led to the development of TESTA,[50] a European network connecting the national networks of member states' administrations. The Commission, with the member states, now wishes to create a security policy for TESTA, to specify the technical and operational conditions for interconnecting TESTA with the national networks and to set up an approval procedure for TESTA that involves the national partners.

Security of the Galileo *satellite navigation programme*

In its resolution of 19 July 1999, the Transport Council decided to entrust the Commission, in collaboration with the European Space Agency, with the task of leading a study to define the *Galileo* satellite navigation programme. Not only was this the first space programme undertaken under this framework, but above all Galileo was related to front-line security issues – accurate localisation, navigation and synchronisation signals available everywhere – and can be a major asset in controlling a crisis situation, but also a great danger if it falls out of control and into the hands of hostile groups. Some information on system characteristics had to be protected from the outset, and a security regulation was adopted for the Commission on 30 November 2001 so that information exchanges with industrialists and the representatives of the member states could be protected.

The decision to develop and actually deploy this programme now raises the question of the operational management of these security issues, in particular the decision-making process, which has to be very fast in time of crisis. For example, on what grounds can some signals be weakened, made inaccessible to some users or eliminated? The authority responsible for analysing a crisis situation, for taking the appropriate decisions without delay and for

49. Interoperable Delivery of pan-European eGovernment services to public Administrations, Businesses and Citizens (IDABC).

50. Trans-European Services for Telematics between Administrations.

getting the system operator to apply them, can only be at the European level and outside the usual mechanisms of decision preparation within the Union. It is clear now that this front-line operational responsibility will fall, in one form or another, to the EU Council and the High Representative for CFSP. The latter will be supported by the Centre for security and safety,[51] which was defined in the regulation setting up the Galileo supervisory authority.[52]

Protection of classified information

Through the Treaty of Nice, the European Union inherited the WEU's WEUnet operating network, which connects the Secretariat of the Council with the capitals of member states. This was merged with the Cortesy network, which connects the 25 foreign ministries, the permanent representatives, the Commission and the Secretariat of the Council in Brussels, and was renamed ESDPnet. It now has to provide a high-level security link between EU staff headquarters and Operational Headquarters in the event of an engagement of forces. To develop this network and make it operational, the General Secretariat of the Council has been confronted with three new problems. It has to:

- adopt and implement an internal security regulation to protect classified information;
- set rules that allow all member states to acknowledge the quality of a government facility produced by one of them;
- make an agreement with NATO on the rules for protecting classified information issued by one or other organisations.

A security regulation was adopted for the Secretariat of the Council on 31 March 2001. Attached to the General Secretariat of the Council, but distinct from the Security Office, an Infosec Office has been created. By the end of 2004, it was due to encompass half a dozen Infosec experts, enabling the General Secretariat of the Council to become a full partner in the management of classified information on the basis of rules of equivalence with the classified information of the member states. The Infosec Office activities are supervised by an Infosec Committee consisting of member states' representatives and chaired by the Head of the Infosec Office.

The CISPS (Council Infosec Selection and Procurement Scheme), adopted in December 2002, is a procedure for issuing

51. See 'State of advancement of the Galileo research programme at the start of the year 2004', COM(2004), 112 final, Brussels, 18 February 2004.

52. Council regulation (EC) no. 1321/2004 of 12 July 2004, Articles 2 and 22.

calls for tenders and assessing and accepting equipment developed by one member state for the handling of classified information on the networks of the Council of the EU. It is based, in particular, on the appointment of national AQUAs (Appropriately Qualified Authorities) responsible for assessing equipment provided by an industrialist from another member state, and if necessary in the presence of representatives of the latter. The final choice between the equipment that meets the originally agreed criteria (Minimum Technical Characteristics) falls to the General Secretariat of the Council.

On 14 March 2003, NATO and the EU signed the NATO-EU Athens accord on Infosec, opening the door to classified information exchanges between the two organisations in order to improve crisis management coordination and to facilitate the transfer of leadership for peacekeeping operations. This accord was complemented on 3 June 2003 by the definition of common standards for the protection of classified information, including equipments that use cryptography.

Since then, NATO and the EU have started discussions with the aim of setting up a mutual recognition agreement on the evaluation and approval of cryptographic equipments used to protect the information they exchange, up to 'secret' level. Such an agreement will be a remarkable extension of the mutual recognition agreement for the evaluation/certification of information and communication technologies from which this type of equipment was exempt (see 2.2).

Protection of critical information infrastructures that have transboundary effect

Following the 'Declaration on combating terrorism' dated 29 March 2004, the European Council in June 2004 asked the Commission and the Secretary General/High Representative for Common Foreign and Security Policy to prepare an overall strategy to protect critical infrastructures. This gave rise to a communication[53] proposing that, according to the subsidiarity principle, EU-level efforts are to concentrate on critical infrastructures that have a transboundary effect, letting the others fall under the sole responsibility of the EU member states using a common framework (see 2.4, last paragraph). In practice, this communication sketches a European Programme for Critical Infrastructure Protection (EPCIP) aimed at reaching adequate levels of security

53. 'Critical Infrastructure protection in the fight against terrorism', Communication from the Commission to the Council and the European Parliament, COM(2004), 702 final, Brussels, 20 October 2004.

for critical infrastructures across the Union, notably thanks to tested recovery contingency plans. A preliminary step could be to set up, as early as 2005, a Critical Infrastructure Warning Information Network (CIWIN) made up of EU member state CIP specialists in order to promote the exchange of information on shared threats and vulnerabilities and to identify measures and strategies for enhancing CIP.[54]

The European Network and Information Security Agency (ENISA)

The growing importance of security issues in Europe and the need to improve information sharing and cooperation between the national initiatives in this domain led the Council and the Parliament, at the beginning of 2004, to approve the creation of a European agency responsible for network and infosec (ENISA).[55] With a budget of €33 million and a staff of about 50, its main objective is to promote the development of a culture of network and Infosec within the EU.

The role of ENISA will therefore be to act as a centre of expertise '*[capable] of assisting the Commission, the Member States, and in consequence cooperating with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the internal market*'. In particular it will have to '*enhance cooperation between different actors operating in the field of network and information security … by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies*'. One of its first tasks will be to draw up an EU-wide skills catalogue of all the professions and actors involved in Infosec.

Apart from raising awareness and '*promoting exchanges of current best practice, including on methods of alerting users*', ENISA will have to '*advise the Commission on research in the area of network and information security*' and '*track the development of standards for products and services on network and information security*'. On the other hand, its area of competence in no way applies to activities related to '*public security, defence, State security and the activities of the State in areas of criminal law*'. It remains limited to the Lisbon strategy and does not include operational activities or direct participation in the fight against computer-related crime. Finally, ENISA should launch short- or long-term analysis on current and emerging risks, thus enhancing

54. See Gustav Lindstrom, 'Critical Infrastructures in Europe', *Chaillot Paper* (forthcoming).

55. Regulation (EC) no. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. See also Council resolutions 2002/C 43/02 (29 January 2002) and 2003/C 48/01 (18 February 2003) as important milestones on the road to establishment of ENISA.

the comprehension of network and information issues, but is not expected to act like a CERT (see above) in the resolution of day-to-day incidents.

It is clearly too early to appreciate the role ENISA will play in the development of Infosec policies across Europe and beyond. The year 2005 should mainly be devoted to the implementation of the agency in Heraklion (on the Greek island of Crete), the recruitment of experts, the evidence of its capacity in the fields of security awareness raising, the organisation of dialogues between the different partners and stakeholders, and the consolidation of its technical expertise in the field of information and network security.

However, sooner or later, ENISA should become an important actor for Infosec policy in the EU, and contribute to the reduction of the disparities within or between the member states' technical and operational capabilities. In that sense, ENISA is expected to play a major role in the improvement of the general Infosec level throughout the EU.

Towards an ambitious and coherent Infosec policy in Europe

Starting from remote positions, the national and European Infosec policies have rapidly evolved towards each other.

Initially, national policies were based on the primacy of intelligence and the restricted use of cryptography; however, they have evolved to meet the need for confidence and security regarding all socio-economic exchanges in the high performance information society that Europe and the member states are striving to build. Given the different socio-economic players, wider access to tools and services that offer high levels of security for all their exchanges goes hand-in-hand with a strengthening of the capacity to combat criminal acts. National policies are differentiated now by the relative weight of their different components and the different degrees to which they are integrated institutionally, technologically, and methodologically.

The EU, in contrast, has no history in the intelligence field and is continuing to pursue its economic and monetary policies on the basis of the rights of individuals and on economic competition regulations. However, the Union is today facing IT-related constraints in the development of ESDP.[56] Infosec has become a dual theme and the Union's operational responsibilities are increasing substantially.

56. Javier Solana, 'A secure Europe in a better world. European Security Strategy', document adopted at the European Council, Brussels, 12 December 2003, p. 5.

The interaction of these two thrusts, at the national and European level, is at the heart of the question of the respective prerogatives of member states and the Union in this area, now and in the future.

Answers to the following questions may cast some light on the future, and on the issues to be faced, several questions may now give us some pause for thought.

- *Must the Infosec industry be considered a strategic one?* Recent history, marked by increasing deregulation in the delivery and use of cryptography (even following the attacks of 11 September 2001) does not seem to have evolved in that direction. However, monopolies in information and communication technology do not just have economic risks, but also security implications for businesses and the state apparatus. Therefore they should lead to clearly defined industrial policies on the maintenance of diversity in supply, action in favour of open source software, support for innovation, etc.
- *Is Internet governance a major issue in respect of the security and strategic autonomy of states?* The current Internet management method, through the ICANN[57] with which the United States maintains a special link, is one of the points being discussed in the framework of the World Summit on the Information Society. The imminent deployment of the Internet protocol IPv6 must not increase centralisation of the name assignment system or reduce the digital sovereignty of states.
- *How can operational coordination throughout Europe be improved, particularly in the field of vigilance, warning and protection of critical infrastructures?* The classic context is that of relations between a ministry in charge and an infrastructure operator. But deregulation is encouraging the fragmentation of infrastructures, the growing number of operators and the deployment of some of them at a European level. At the same time, the threats are becoming cross-border in nature. Moreover, the sharing and the complementary nature of responsibilities between the public and the private sector are not perceived in the same way among the member states, while the need to combat terrorism calls for more coordination at the European level;
- *What will be the role and importance of Infosec for the military capabilities of ESDP?* The emerging procedures for coordinating the capabilities of member states in order to build secure information systems in the Union, such as ESDPnet, represent a prag-

57. Internet Corporation for Assigned Names and Numbers. Due to its role as successor of IANA (Internet Assigned Numbers Authority), ICANN has maintained a special relationship with the US government through a Memorandum of Understanding (MOU) reached between ICANN and the US Department of Commerce in November 1998 (the parties agreed to work jointly on a series of tasks necessary to complete the privatisation, see http://http://www.icann.org/general/icann-mou-25nov98.htm) and two subsidiary agreements: a Cooperative Research and Development Agreement (CRADA) for enhancements to the root-name server system and a contract for operation of the IANA (see http://http://www.icann.org/announcements/icann-pr04sep00.htm). The US government has also repeatedly blocked initiatives that could result in a loss of power over ICANN, in particular attempts of the ITU (International Telecommunications Union) to take over responsibility for the technical coordination and management of the Internet domain system (see http://www.icannwatch.org/article.pl?sid=04/10/041851217).

matic response to a pressing need but do not shed any light on the role of Infosec in the Union's military strategy, or for its future military needs.

These four questions implicitly bring us back to the more general question of an overall European doctrine on the value of information as a vector for the development of society and the management of its major issues, starting with security. It also returns us to the question of how to organise exchanges of intelligence within the Union,[58] something that is now of even greater urgency following the attacks of 11 March 2004 in Madrid.

Faced with the development of information and communication technologies, the United States has responded by developing the paradigm of 'information dominance', implying as it usually does the primacy of technology and ambiguities over industrial or political relations with allied countries. It is no longer a question of approving or condemning this paradigm, but rather of working on the questions above, in order to try and clarify which route Europe is to take between 'information dominance' and 'information dependence'.

58. Björn Müller-Wille, 'For our eyes only? Shaping an intelligence community within the EU', *Occasional Paper* 50 (Paris: EU Institute for Security Studies, January 2004).

Conclusion

Thanks to its wide range of applications and enormous commercial success, the Internet has become the spinal column of modern societies, and its importance will certainly continue to increase. However, Internet protocols have been defined in order to improve the rapidity and interoperability of electronic exchanges, not their security. The spread of a system that is pathologically insecure to all sectors of society has thus created new security risks that are impossible to eliminate completely.

Although its development has been – and will continue to be – driven mainly by private businesses, public authorities also have, for a variety of reasons, an important responsibility concerning the use of cyberspace.

- The Internet can affect collective and personal security, the provision of which is traditionally the primary duty of states. Governments therefore have a specific role to play in the management of the Internet's security implications. This concerns a broad spectrum of areas, ranging from the protection of personal data to the protection of critical infrastructures.
- Local, regional, national and international authorities increasingly take advantage of the Internet as well. As part of public sector reform, e-government helps public services to reduce costs and become more efficient, both internally and vis-à-vis citizens. The public sector itself thus represents an important user community and must therefore define its own Infosec priorities and policies so as to manage its increasing dependence on the Internet.
- In particular at the national and international level, authorities must master their communications means if they are to maintain their autonomy of decision and action. In order to fully exploit the advantages of electronic communication, they must ensure the confidentiality and integrity of the latter.

However, all this is easier said than done, since there is a structural mismatch between security, which is still a national domain, and cyberspace, which is transnational in nature, global in reach and outside any state control. In consequence, the Internet's security implications can only be tackled through international cooperation and close partnership between public and private sectors. The following points seem particularly important.

- *Internet governance* is a highly controversial issue and illustrates the difficulties in coping with the challenges of globalisation. This is true in particular of its political dimension. However, various international forums have launched initiatives to make cyberspace more secure (UN, G-8, Council of Europe, EU). In this context, the Convention on Cybercrime is particularly important, since it is the first international treaty in this area. All signatories should do their best to implement these provisions rapidly and to convince as many countries as possible to subscribe to them. Moreover, the current discussion on the organisation and administration of the Domain Name System, including the operation of the DNS root servers, must take into account public interest concerns and aim at an internationalisation of Internet governance.
- *Infosec culture and practice*. The development of a culture and practice of network and Information security must be strongly encouraged through campaigns to increase awareness, tutoring and online training modules, operational exercises, etc. The OECD Guidelines for the Security of Information Systems and Networks provide an appropriate framework for action in this field and should therefore be followed closely. To be effective, awareness activities should be tailored to the specific needs of different user groups (businesses, public services, citizens, etc.).
- *Infosec management*. Along these lines, there must be a systematic risk analysis throughout the development, implementation and administration of information networks, with a clear share of responsibility between the stakeholders (governments, providers, operators, citizens). This also includes the development of Infosec master plans for specific information networks and crisis management planning, notably for cyberattacks on critical infrastructures. In this context, the ability of CSIRTs and CERTs to cooperate efficiently, in particular to tackle possible attacks against transnational networks, is crucial.

- *Procurement diversity*. On most IT markets, non-European monopolies are a matter of fact. The challenge will be to manage their negative consequences. In particular in sensitive areas like encryption and authentication, public authorities must have security of supply for dependable equipment. This supposes systematic evaluation of products and reliable relations with producers. On top of this, it may also imply measures to maintain certain industrial and technological capabilities, for example through R&D programmes and specific innovation incentives.
- *Product evaluation*. For governmental products, high-level security evaluation and certification is possible, since mathematical models of proof are in general used in the design and development phases. For the development of most commercial products, on the other hand, security is not adequately taken into account. Possible security gaps are discovered (and partially resolved) only after products have been put on the market. To change this and allow for evaluation up to a high level of security, public authorities should offer strong incentives for industry to improve its product development and testing procedures. They could also use their (considerable) purchasing power to achieve this objective.

All this is of relevance for the European Union as well, and the Union can play an important role in making cyberspace more secure. As we have seen, the EU is already an established actor in the field of Information Technology, but is only just beginning to tackle its security dimension seriously. Given the importance of IT for all sectors, Infosec should clearly become an integral part of the EU's comprehensive security approach. This also implies a clear definition of what the EU itself can contribute to overall Infosec in Europe. In accordance with the above-mentioned priorities, the following points could serve as guidelines for EU action.

- The EU should put Internet governance on its agenda of effective multilateralism. Member states should not only be the first to implement internationally agreed Conventions, they should work together to convince others to sign up to and implement them. Using the EU as the framework for action would strengthen Europe's voice in the world, and in particular vis-à-vis the United States, which is by far the most important 'cyber-power'.

- The more comprehensive security becomes, the greater the variety of EU bodies that have to deal with security-relevant information. The EU therefore needs to develop an Infosec policy for its own services, including security management and culture, with commonly agreed security standards and best practices (product evaluation, procurement policies and internal awareness programmes).
- At the same time, the EU can also provide a useful framework for supporting and coordinating member states' activities. Through its community policies in particular, it can contribute to strengthening Europe's industrial and technology base in this field and help to ensure a consistent level of Infosec throughout the Union. In this context, awareness campaigns such as INSAFE[1] are particularly important and should be further developed.

There are a variety of existing and planned EU initiatives, which illustrates a growing recognition of the importance of Infosec. ENISA in particular may give some valuable impetus in a number of these issues, notably Infosec culture and practice, R&D orientations, awareness programmes, etc. In parallel, the future European Security Research Programme will be able to make an important contribution to information and network security. However, both initiatives must be sufficiently funded to make their weight felt.

Last but not least, coordination is crucial. There is today, not surprisingly, a lack of coherence between the various activities that leaves plenty of room for deepening discussions between stakeholders. Again, the Union seems to be an appropriate forum in which to organise and structure such a debate, which could finally lead to a White Paper on a European Infosec policy.

1. http://www.eun.org/eun.org2/eun/en/about_ewatch/content.cfm?lang=en&ov=33951.

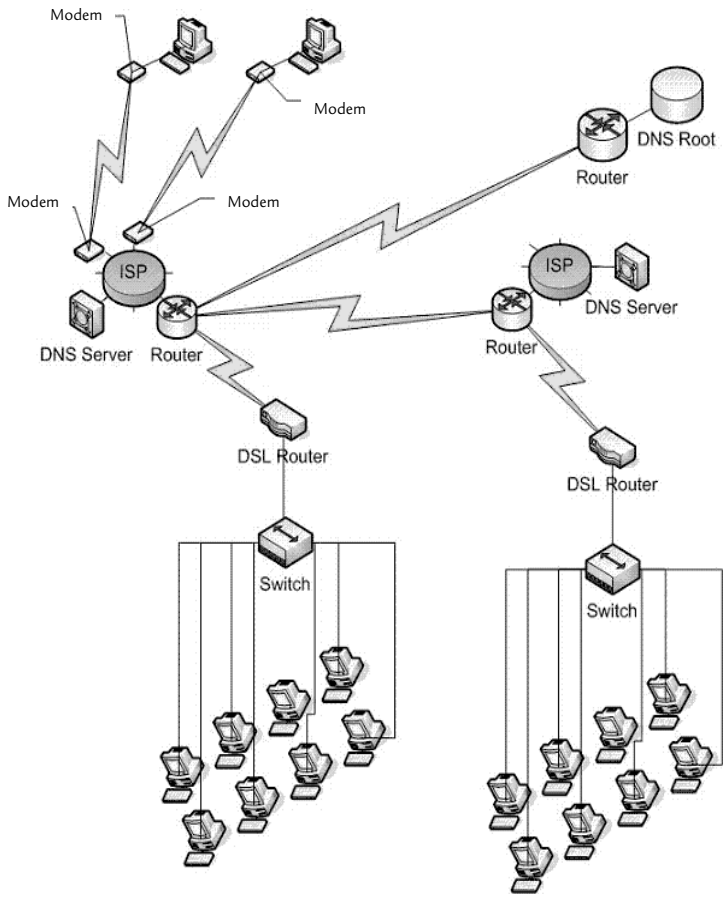
About the authors

Alain Esterle. After working for 25 years on space programmes and policies, he moved to the French defence ministry in 1995 where for four years he was involved in the adaptation of the French military to the new international and European context. With a background in engineering and science policy, in 2000 he joined the General Secretariat for National Defence (SGDN) as deputy director of the central directorate for information system security (DCSSI). He has played a leading role in forming national IT security policy and currently in its inter-ministerial implementation. He is currently alternate member of the European Network and Information Security Agency (ENISA).

Hanno Ranck heads the Communications and Information Technology Department at the European Union Institute for Security Studies. He has a law degree from the University of Hamburg, with specialisation in media law. He previously worked as a producer and editor for AOL Time Warner and as an independent consultant on projects for Deutsche Telekom, Helicon Management Consultants and the WEU Institute for Security Studies.

Burkard Schmitt has a Doctorate in contemporary history from the Friedrich Alexander University Erlangen/Nürnberg, and a Master's degree from the University of Bordeaux. From 1995 to 1998, he worked as an independent researcher, consultant and journalist. From 1998 to 2001, he was research fellow at the WEU Institute for Security Studies. Since 2002, he has acted as Assistant Director at the EUISS. His main research areas are defence industries and armaments cooperation.

Simplified diagram of the Internet



DNS Server: short for Domain Name System Server, an Internet server that translates domain names into IP addresses. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

DNS Root Server: a system of 13 file servers that are distributed around the globe and contain authoritative databases that form a master list of all top-level domain names (TLDs).

DSL: DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

ISP: short for Internet Service Provider, a company that provides access to the Internet.

Modem: short for modulator-demodulator. A modem is a device or program that enables a computer to transmit data over, for example, telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analogue signals. A modem converts between these two forms

Router: a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.

Switch: a device that filters and forwards data packets between LAN segments. Switches operate at the data link layer and sometimes the network layer of the Internet Protocol Suite and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

OECD guidelines for the security of information systems and networks

Towards a culture of security

PREFACE

The use of information systems and networks and the entire information technology environment have changed dramatically since 1992 when the OECD first put forward the *Guidelines for the Security of Information Systems*. These continuing changes offer significant advantages but also require a much greater emphasis on security by governments, businesses, other organisations and individual users who develop, own, provide, manage service and use information systems and networks ('participants').

Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through 'always on' connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these Guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a 'culture of security'.

I. Towards a Culture of Security

These Guidelines respond to an ever changing security environment by promoting the development of a culture of security – that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks. The Guidelines signal a clear break with a time when secure design and use of networks and systems were too often afterthoughts. Participants are becoming more dependent on information systems, networks and related services, all of which need to be reliable and secure. Only an approach that takes due account of the interests of all participants, and the nature of the systems, networks and related services, can provide effective security.

Each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks.

Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants. These Guidelines constitute a foundation for work towards a culture of security throughout society. This will enable participants to factor security into the design and use of all information systems and networks. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.

II. Aims

These Guidelines aim to:

- Promote a culture of security among all participants as a means of protecting information systems and networks.
- Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures avail-

able to address those risks; and the need for their adoption and implementation.

- Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.
- Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
- Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

III. Principles

The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy.[1]

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others

arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics

Participants should respect the legitimate interests of others.

Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or

inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the

organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

Recommendations of the Council concerning guidelines for the Security of information systems and networks

Towards a culture of security

THE COUNCIL,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, Articles 1 b), 1 c), 3 a) and 5 b) thereof;

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

Having regard to the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

Having regard to the Recommendation of the Council concerning Guidelines for Cryptography Policy of 27 March 1997 [C(97)62/FINAL];

Having regard to the Ministerial Declaration on the Protection of Privacy on Global Networks of 7-9 December 1998 [Annex to C(98)177/FINAL];

Having regard to the Ministerial Declaration on Authentication for Electronic Commerce of 7-9 December 1998 [Annex to C(98)177/FINAL];

Recognising that information systems and networks are of increasing use and value to governments, businesses, other organisations and individual users;

Recognising that the increasingly significant role of information systems and networks, and the growing dependence on them for stable and efficient national economies and international trade and in social, cultural and political life call for special efforts to protect and foster confidence in them;

Recognising that information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks;

Recognising that data and information stored on and transmitted over information systems and networks are subject to threats from various means of unauthorised access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards;

Recognising that there is a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond to those risks, and to encourage appropriate behaviour as a crucial step towards the development of a culture of security;

Recognising that there is a need to review current policies, practices, measures, and procedures to help assure that they meet the evolving challenges posed by threats to information systems and networks;

Recognising that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life;

And further recognising that the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations;

And recognising that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security;

COMMENDS these *Guidelines for the Security of the Information Systems and Networks: Towards a Culture of Security* to governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks;

RECOMMENDS that Member countries:

Establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* by adopting and promoting a culture of security as set out in the Guidelines;

Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines;

Disseminate the Guidelines throughout the public and private sectors, including to governments, business, other organisations, and individual users to promote a culture of security, and to encourage all concerned parties to be responsible and to take necessary steps to implement the Guidelines in a manner appropriate to their individual roles;

Make the Guidelines available to non-member countries in a timely and appropriate manner;

Review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to promote the implementation of the Guidelines.

This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL].

Procedural History

The Security Guidelines were first completed in 1992 and were reviewed in 1997. The current review was undertaken in 2001 by the Working Party on Information Security and Privacy (WPISP), pursuant to a mandate from the Committee for Information, Computer and Communications Policy (ICCP), and accelerated in the aftermath of the September 11 tragedy.

Drafting was undertaken by an Expert Group of the WPISP which met in Washington, DC, on 10-11 December 2001, Sydney on 12-13 February 2002 and Paris on 4 and 6 March 2002. The WPISP met in Paris on 5-6 March 2002, 22-23 April 2002 and 25-26 June 2002.

The present *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.

G8 Principles for protecting critical information infrastructures

Information infrastructures form an essential part of critical infrastructures. In order effectively to protect critical infrastructures, therefore, countries must protect critical information infrastructures from damage and secure them against attack. Effective critical infrastructure protection includes identifying threats too and reducing the vulnerability of such infrastructures to damage or attack, minimizing damage and recovery time in the event that damage or attack occur, and identifying the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement. Effective protection also requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies. Such efforts should be undertaken with due regard for the security of information and applicable law concerning mutual legal assistance and privacy protection.

To further these goals, we adopt the following PRINCIPLES and encourage countries to consider them in developing a strategy for reducing risks to critical information infrastructures:

I. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.
II. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.
III. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.
IV. Countries should promote partnership among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.
V. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

VI. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.

VII. Countries should facilitate tracing attacks on critical information infrastructures and, when appropriate, the disclosure of tracing information to other countries.

VIII. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

IX. Countries should ensure that they have adequate substantive and procedural laws, such as those described in the Council of Europe Cybercriminality Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.

X. Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities, threats and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

XI. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

Extract from NICSS Quarterly, 02/03; http://www.niscc.gov.uk/ Quarterly/NQ_APRIL03_JUNE03.pdf.

Abbreviations

ADAE	Agence pour le Développement de l'Administration Electronique
APNIC	Asia/Pacific Network Information Center
AQUA	Appropriately Qualified Authorities
ARIN	North American Registry for Internet Numbers
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
BIOS	Basic Input Output System
BKI	BundesKriminalamt, Germany
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPS	CESG Assisted Products Scheme
CC-MRA	Common Criteria Mutual Recognition Arrangement
CCN	Centro de Criptologia Nacional/National Cryptology Centre
CCRC	Computer Crime Research Center
CCU	Computer Crime Unit
CERN	European Organization for Nuclear Research
CERT	Computer Emergency Response Team
CESG	Communications Electronics Security Group
CFSP	Common Foreign and Security Policy
CI	Critical Infrastructure
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CISPS	Council Infosec Selection and Procurement Scheme
CIWIN	Critical Infrastructure Warning Information Network
CNI	Centro Nacional de Intelligencia
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies
CSP	Certification Service Providers
DACAN	Military Committee Distribution & Accounting Agency, NATO
DARPA	Defence Advanced Research Projects Agency
DCCP	Datagram Congestion Control Protocol
DCS	Distributed Control Systems
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DDoS	Distributed Denial of Service
DGA	la Délégation Générale pour l'Armement
DNS	Domain Name Service/Server
DSL	Digital Subscriber Line
DTI	Department of Trade and Industry (UK)
EADS	European Aeronautic Defence and Space Company
EAL	Evaluation Assurance Level
ECAP	European Capabilities Action Plan
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection

ESDP	European Security and Defence Policy
ESRP	European Security Research Programme
ETA	Basque Fatherland and Liberty
FBI	Federal Bureau of Investigation
FDDI	Fiber Distributed Data Interface
FESA	Forum of European Supervisory Authorities for Electronic Signature
FP	Framework Programme
FTP	File Transfer Protocol
GCHQ	Government Communications Headquarters
GISS	General Intelligence and Security Service
GoP	Group of Personalities
GPRS	General Packet Radio Service
GSP	Government Security Program
HTTP	HyperText Transfer Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
ICCP	Information, Computer and Communications Policy
ICS	Industrial Control Systems
IDA	Interchange of Data between Administrations
IDABC	Interoperable Delivery of pan-European eGovernment services to public Administrations, Businesses and Citizens
IDC	International Data Corporation
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPTS	Institute for Prospective Technological Studies
IPX	Internetwork Packet Exchange
IRA	Irish Republican Army
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ISP	Internet Service Providers
IST	Information Society Technologies
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
JHA	Justice and Homeland Affairs
LACNIC	Latin and Central American Network Information Center
LAN	Local Area Network
LTTE	Liberation Tigers of Tamil Eelam

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NCP	National Contact Point
NHTCU	National High Technology Crime Unit
NIISC	National Information Infrastructure Steering Committee
NISCC	National Infrastructure Security Coordination Centre
NIST	National Institute for Standards
NLNCSA	Nederland National Communication Security Agency
NSA	National Security Agency
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication
OECD	Organisation for Economic Cooperation and Development
OHQ	Operational Headquarters
PASR	Preparatory Action on Security Research
PCRD	Programme Cadre de Recherche et Démonstration
PKI	Public Key Infrastructures
PKK	Kurdistan Workers Party
R&D	Research and Development
RIPE-NCC	Réseaux Internet Protocol Européens-Network Coordination Centre
RTP	RealTime Transport Protocol
SCADA	Supervisory Control and Data Acquisition
SCTP	Stream Control Transmission Protocol
SGDN	Secrétariat Général de la Défense Nationale
SIGINT	Signal Intelligence
SME	Small and Medium-sized Enterprises
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
STOA	Scientific and Technological Options Assessment
TCP	Transmission Control Protocol
TEMPEST	Test for Electromagnetic Propagation and Evaluation for Secure Transmissions/Transient ElectroMagnetic PulsE STandard
TENs	Trans-European Networks
TERENA	Trans-European Research and Education Network Association
TESTA	Trans-European Services for Telematics between Administrations
TF-CSIRT	Task Force-CSIRT
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UNIRAS	Unified Incident Reporting and Alert Scheme
W3C	World Wide Web Consortium
WARP	Warning, Advice and Reporting Point
WEU	Western European Union
WPISP	Working Party on Information Security and Privacy

European Union Institute for Security Studies

Luxembourg: Publications Office of the European Communities

2005 - 78 pp. - 17x24cm

ISSN 1017-7566
ISBN 92-9198-069-2

Printed in Luxemburg

PRINTED ON WHITE PAPER WITHOUT BLEACH

Chaillot Papers

All *Institute publications*
can be accessed via the Institute's website:
www.iss-eu.org

n°75 EU security and defence. Core documents 2004 — **February 2005**
Volume V

n°74 What Russia sees — **January 2005**
Dmitry Danilov, Sergei Karaganov, Dov Lynch, Alexey Pushkov, Dmitri Trenin and Andrei Zagorski; edited by Dov Lynch

n°73 Afghanistan : la difficile reconstruction d'un Etat — **Décembre 2004**
Olivier Roy

n°72 Global views on the European Union — **November 2004**
Amitav Acharya, Marcel F. Biato, Babacar Diallo, Francisco E. González, Toshiya Hoshino, Terence O'Brien, Gerrit Olivier and Yi Wang; edited by Martin Ortega

n°71 La cohérence par la défense. Une autre lecture de la PESD — **Octobre 2004**
Philippe de Schoutheete

n°70 The Western Balkans: moving on — **October 2004**
Franz-Lothar Altmann, Judy Batt, Misha Glenny, Gerald Knaus and Marcus Cox; Stefan Lehne, Jacques Rupnik, Ivan Vejvoda and Romana Vlahutin; edited by Judy Batt

n°69 Protecting the European homeland: the CBR dimension — **July 2004**
Gustav Lindstrom

n°68 One year on: lessons from Iraq — **March 2004**
Ron Asmus, Christoph Bertram, Carl Bildt, Esther Brimmer, Marta Dassú, Rob de Wijk, James Dobbins, William Drozdiak, Nicole Gnesotto, Philip H. Gordon, Charles Grant, Gustav Gustenau, Pierre Hassner, John Hulsman, Atis Lejins, Catherine McArdle Kelleher, Andrew Moravcsik, Janusz Onyszkiewicz, Jiri Sedivy, Narcis Serra and Alvaro Vasconcelos; edited by Gustav Lindstrom and Burkard Schmitt

Books

EU Security and Defence Policy — the first five years (1999-2004) — **2004**
Martti Ahtisaari, Michel Barnier, Carl Bildt, Elmar Brok & Norbert Gresch, Robert Cooper, Judy Dempsey, Lamberto Dini, Jean-Louis Gergorin & Jean Bétermier, Philip H. Gordon, Jean-Yves Haine, Gustav Lindstrom, Antonio Missiroli, Alberto Navarro, Martin Ortega, Ferdinando Riccardi, Alexander Rondos, Burkard Schmitt, Rainer Schuwirth, Theo Sommer and Laurent Zecchini; edited by Nicole Gnesotto; preface by Javier Solana

European defence — a proposal for a White Paper — **2004**
André Dumoulin, Jan Foghelin, François Heisbourg, William Hopkinson, Marc Otte, Tomas Ries, Lothar Rühl, Stefano Silvestri, Hans-Bernhard Weisserth, Rob de Wijk; Chair: Nicole Gnesotto, Rapporteur: Jean-Yves Haine

Shift or Rift — assessing US-EU relations after Iraq — **2003**
Nicole Gnesotto, Stanley Hoffmann, Antonio Missiroli, David Gompert, Jean-Yves Haine, Ivo Daalder, James Lindsay, Martin Ortega, Patrick Clawson, Dimitrios Triantaphyllou, Daniel Serwer, Gustav Lindstrom, Brian Jenkins; edited by Gustav Lindstrom

QN-AA-05-076-EN-C

The Internet has opened a new area of communication and information, enabling us to transfer enormous amounts of digital data for a great variety of applications within fractions of a second around the globe. It is therefore no surprise that it has become, within only a few years, the spinal column of modern societies. Citizens, research institutions, private business, NGOs, political parties and public services all increasingly depend in their daily life and work on interlinked information systems and networks.

Dependency, however, creates vulnerabilities and risks. Given its enormous success, disruption of the Internet – even temporary – can cause tremendous economic and financial damage. At the same time, the Internet can be misused as an instrument for all kind of criminal activities, be they economically or politically motivated. Cybercrime and cyberterrorism have thus become serious threats to the security of our society.

This *Chaillot Paper* explains the security risks that modern information systems incur, and the various attempts of the European Union and its member states to cope with these risks. Its has two objectives.

The first is to raise awareness: among all those who use the Internet regularly for professional reasons without a full understanding of the dangers involved, but also among decision-makers who still tend to underestimate the enormous economic and political dimension of cyberspace and its related risks.

The second objective is to explore options for further European cooperation. Since the Internet's security implications are necessarily transnational, no member state can tackle them individually. There is thus an urgent need to develop a comprehensive and fully-fledged European policy on information security, both to protect our citizens at home and to increase Europe's influence when decisions are taken on how to organise and protect the Internet as a truly global tool.

EU Institute for Security Studies

www.iss-eu.org

€ 10

Publications Office
Publications.eu.int

ISSN 1017-7566
ISBN 92-9198-069-2