

## **Part I**

### **Problem and context**

## Chapter 2. An information society needs information security

*The future had arrived. There was a generation waiting to inherit the earth, caring nothing for old-timers' concerns: dedicated to the pursuit of the new, speaking the future's strange, binary, affectless speech—quite a change from our melodramatic garam-masala exclamations.*

*(Salman Rushdie, The Moor's Last Sigh)*

At the threshold of a new millennium, a new society is emerging: the information society. As more and more people rely on information for their work, entertainment, and daily life, information and communication technologies conquer large parts of society. The protection of these areas of life must be redefined, then, in terms of information security. Particularly the confidentiality, integrity, and availability of information should be safeguarded. In this chapter, I will sketch the outlines of the information society – (inter)national policies, the infrastructure, and the problems confronting it (2.1). Then, I will describe the role of information security therein (2.2). I will pay particular attention to the role of governments in establishing information security.

### 2.1. The information society

Europe's citizens and consumers can look forward to a more caring European society with a significantly higher quality of life. Thus spoke the Bangemann Report on *Europe and the global information society* [Bangemann 94]. The information revolution will profoundly change the way we live and work.<sup>1</sup>

#### 2.1.1. Developments

Several developments contribute to the emergence of this information-based society. First, information is increasingly being digitized through the enhancement of information technol-

---

<sup>1</sup> Information and communication technologies are affecting almost all professions. For instance, a farmer nowadays relies on computers for his increasingly complex paperwork and for production planning, while he uses telecommunications to increase his action radius. A well-known example is the Texas rancher who gave his cows pagers rather than bells, and they would gather at the right place when beeped. [Telemanagement, February 1995] The issue of the changes in work through information and telecommunication technologies (teleworking, employment shifts, and changing job profiles) is specifically addressed in the report *Building the European information society for us all* of January 1996, by a high-level group of senior experts of the European Union which investigates the social and societal aspects of the information society.

ogies. As the cost-performance ratio of these technologies is dropping, the advantages of digitizing information are rapidly becoming clear. It can be processed at astounding speeds, reproduced without any effort, and spread over large distances in an instant. Moreover, interfaces for information processing have become much more user-friendly; for instance, the Internet really started to be used on a large scale after the advent of its graphic interface, the World Wide Web (WWW).

A second development is the increasing integration of different media. Whereas, for instance, telephones and computers used to perform different functions, information technologies and telecommunications technologies nowadays increasingly interoperate; thus, one speaks of information and communication technologies (ICT). Telephone lines are being used for facsimile traffic, electronic data interchange, and e-mail, and Internet technology can be used for making cheap long-distance phone calls. The market for telematics, the combination of telecommunications and information technology, is soaring. Television cable networks have a huge potential for carrying all kinds of information, with the possibility of interactive communications – a great advance over the one-way broadcasting of television programs. Ultimately, an integration of computer, television, telephone, and facsimile might be expected.

A third and related development is the convergence of sectors. Where formerly the sectors of telecommunications infrastructure, telecom services, and content were clearly separated, increasingly companies occupy themselves with several segments of the ICT market at one and the same time. For instance, telephone companies offer network and value-added services. Cable network operators merge with service providers and busy themselves with providing content. Some operating-systems producers even want to have a say in every ICT market segment. Thus, in the information society, a new infrastructure is emerging, with new segments and blurred borderlines.

Increasing liberalization of the telecommunications sector contributes to the growing attractiveness of telecommunications. Once the telecom market has been fully liberalized (in the European Union, this was largely the case in January 1998), users can choose from a range of providers and services, which providers will gear to their needs in order to survive in the competitive market. A good illustration is the fast-growing market of mobile phones, where fierce competition has lured numerous people into buying a mobile phone. Apparently, more and more people consider a mobile phone vital<sup>2</sup> (for their status if not for their needs).

Moreover, the information society is primarily demand-driven [23900, nr 20, 2.1]. Due to the proliferation of services, customers can pick and choose what kind of information they want and how and when they want to receive it. Video-on-demand is an example (albeit a slowly developing one); in the near future, knowbots (information agents) may roam the information superhighway to collect specific bits of information their masters are interested in.

The youngest development of the information society is electronic commerce. Industry and governments are beginning to realize the potential of the online economy – ordering,

---

2 A Swede perished on Midsummer eve 1995 when he dived from a ferry to save his mobile phone [Volksskrant, 20 June 1996].

paying, and, with intangible products, delivering through electronic networks. Although everyone recognizes the importance of this development, electronic commerce is yet in its infancy. Lack of consumer trust (in payment systems and the protection of personal data, for instance) and the uncertainty over the legal implications and obligations are among the main obstacles for e-commerce to fully bud and bloom.<sup>3</sup>

Overarching all these developments is the increasingly global nature of the information society. Globalization (or, if you perceive the information society as a global village, glocalization) permeates the information revolution, which causes traditional frontier-based distinctions to be increasingly obsolete. Territoriality gives way to borderless cyberspace. The physical constraints of volume, time, and space are fading, as electronic media displace material applications.

These developments lead to a society that is increasingly dependent on information. An estimated two thirds of the economy in Western countries rely on information-related work,<sup>4</sup> and many functions of the network economy (communication, information management, transactions) rely to a large extent on electronic information exchange [WRR, 7]. This development is so profound that some speak of “a new industrial revolution already as significant and far-reaching as those of the past.” [Bangemann 94, 4n]

### 2.1.2. Information society policy

The rise of the information society has been noticed at government levels. Politicians see a huge potential for the information infrastructure, provided certain conditions are met. They have launched initiatives to set down these conditions and to make sure they are met.

#### United States

US vice-president Gore in 1993 launched the National Information Infrastructure (NII) initiative, which “captures the vision of a nationwide, invisible, seamless, dynamic web of transmission mechanisms, information appliances, content, and people”, in the words of [NIIAC]. Private investment, competition, open access, universal service, and flexible governmental action were seen as key issues. An Information Infrastructure Task Force (IITF) was established, with three committees, on telecommunications policy, information policy, and applications and technology – each divided into working groups that investigate and report on specific subjects. Moreover, an NII Security Issues Forum was established, which coordinates security-related efforts in NII policy. In early 1994, the NII Advisory Council (NIIAC) was set up to advise the administration on a national strategy for promoting the development of the NII and the Global Information Infrastructure (GII). Its first report,

---

3 According to GVU's 8<sup>th</sup> WWW User Survey (endorsed by the World Wide Web Consortium), “security remains the number one reason Web users report for not purchasing over the Web”. [GVU]

4 “Individual, corporate and national wealth expresses itself increasingly in the form of information. The growth and performance of an estimated 2/3 of the economy relies on manufacturing or services heavily dependent on information technology, telecommunications and broadcasting.” [DG XIII, section 1] “[I]nformation is one of America's most critical economic resources, for both service and manufacturing industries, for both economic and national security. This is not surprising, considering the fact that almost two-thirds of US workers have information-related jobs.” [Bekkers, 11-12]

*Common Ground: Fundamental Principles for the NII* of March 1995, presented overall principles for furthering the NII, covering universal access and services, privacy and security, intellectual property, education and lifelong learning, and electronic commerce. It envisioned an improvement of the quality of life, for instance, through strengthening education, improving healthcare, increasing entertainment options, and enhancing participatory democracy, provided the NII is grounded in a unified vision. The 1995 *GII: Agenda For Cooperation* extended the vision of the NII to a global level. [Brown]

Electronic commerce is increasingly seen as a central development in the information society. On 1 July 1997, president Clinton and vice-president Gore presented *A Framework For Global Electronic Commerce*, which suggested a set of principles and presented a series of policies to articulate “the Administration’s vision for the emergence of the GII as a vibrant global marketplace” [Clinton, 3]. The main principles stressed the central starting-point of a non-regulatory, market-oriented approach by governments: the private sector should lead, governments should avoid undue restrictions, and government involvement must aim for a predictable, minimalist, consistent, and simple legal environment. Moreover, electronic commerce over the Internet should be facilitated on a global basis. The ‘non-bureaucratic’ facilitating approach is echoed in the report *The Emerging Digital Economy* of April 1998, one of the elaborations of the Framework [Margherio].

### **European Union**

The May 1994 Bangemann Report *Europe and the global information society – Recommendations to the European Council* confronted the challenge of establishing an information society. Much of it is still as topical today as when it was published. It stressed the need for private investment for developing the information infrastructure, while governments should focus on creating a stimulating and balanced regulatory environment, covering the issues of liberalization,<sup>5</sup> interconnection, universal service, protecting privacy and intellectual property rights, and ensuring free movement in the Internal Market. Furthermore, ten application projects were defined for, among others, teleworking, distance learning, and road-traffic management. The recommendations were elaborated in an action plan by the European Commission, *Europe’s Way to the Information Society* [COM(94) 347], which serves as a reference framework for the EU’s activities on the information society. In 1996, the framework was incorporated into a *Rolling Action Plan* [COM(96) 607].

Three recent EU initiatives relate to the regulation of the information society and specifically of electronic commerce. The EC Communication *A European Initiative in Electronic Commerce* of early 1997 aims to provide a coherent policy framework for Community action in the area of electronic commerce, to encourage “the vigorous growth of electronic commerce in Europe” [COM(97)157]. It calls for a predictable legal and institutional framework to support trust-building technologies, such as digital signatures and electronic payment mechanisms. This was elaborated in the Communication *Ensuring*

---

5 To encourage private investment in the information infrastructure, the telecommunications market was liberalized, a process that started in the 1980s and was completed in early 1998 with the liberalization of the voice telephony market. See [96/19/EC].

*security and trust in electronic communication – Towards a European framework for digital signatures and encryption* of 10 October 1997 [COM(97)503]. The second initiative is the EC Green Paper on convergence of December 1997, which is a discussion paper on the many issues facing the regulatory environment of the information society in view of the increasing convergence of technologies and sectors. It “represents a key element of the overall framework put in place to support the development of an Information Society” [COM(97)623]. On the basis of comments on this Green Paper, the Commission intends to produce a Communication by the end of 1998. The third and most encompassing (and consequently rather vague) initiative is Bangemann’s call for an ‘International Charter’ to coordinate world-wide policies regarding the information society [Bangemann 97, further developed in COM(98)50]. The European Commission argues that the global electronic marketplace requires strengthened international coordination in creating an enabling framework that covers technical, commercial, and legal aspects. The envisaged international charter would not be a detailed document outlining rules on specific topics, but would rather establish a “sustained method of coordination in which public and private sector interests are adequately represented” [COM (98) 50]. The Charter is scheduled to be discussed at a ministerial conference in early 1999.

Europe-wide, at the Bonn conference of 6-8 July 1997, ministers agreed on a reticent role of governments in regulating the information society. A host of representatives from the EU, the EFTA, Central and Eastern Europe, and guests from the US, Canada, Japan, and Russia discussed barriers and solutions to the development of Global Information Networks. The joint declaration affirms that the expansion of global information networks must essentially be market-led. Governments have two major roles: providing a clear and balanced regulatory framework, and stimulating new services. [Bonn]

### **The Netherlands**

National initiatives have followed up and elaborated on the European action plan. The Dutch National Action Plan *Electronic highways: from metaphor to action* [23900, nr 20] of December 1994 and its follow-up reports [24565] stressed the need for additional national activities, in order to strengthen the Netherlands’ position of ‘Gateway to Europe’. The policy was based on two main tiers: liberalizing the telecommunications and media markets to stimulate the private investment needed for establishing a Dutch electronic highway, and redefining the state’s role in the public domain, which changes significantly through the rise of ICT. According to the National Action Plan, the preconditions for a well-functioning information infrastructure should be optimized by addressing such issues as intellectual-property rights, privacy, security, law-enforcement wiretapping, and standardization.

The Dutch government further outlined the issues at stake in regulating the information society in the hefty and somewhat diffuse policy document *Legislation for the electronic highway* of February 1998 [25880, nrs 1-2]. It concluded that the transition to the information society brings far-reaching changes, but does not constitute a radical rupture with the past: offline rules will generally also hold online. The document presents a touchstone for the legislature as well as several suggestions for adapting legislation and regulation. The government defines its main roles as safeguarding fundamental moral values and facilitating electronic traffic. The government notices one major problem “that is not really solvable”:

the international character of the electronic highway. They argue, however, that the problem can be reduced significantly by a 'pragmatic multi-track approach'. Such an approach is similar, one may suppose, to the 'open approach' advocated by the Scientific Council for Government Policy [WRR]. In its 1998 report *State without a territory*, the Council advises to flexibly strike new balances between fundamental points of departure, given the fact that ICT penetration makes obsolete the self-evidence that a state should regulate things based on territoriality. The changes the information society will bring about must not be met in terms of the existing capacity to act and with the customary concepts. 'More-of-the-same' legislation is unlikely to prove sufficient, the report states. (Admittedly, the Council remains somewhat vague about just what new concepts are required in the 'open approach'.)

The touchstone of *Legislation for the electronic highway* lists principles for government intervention. Regulation should preferably be global and involve as many countries as possible, or else be agreed upon in supranational fora such as the OECD, the Council of Europe, or the European Union. National regulation can be considered to protect moral values, if an international approach is not feasible. However, the legislature should first examine whether self-regulation is possible, provided the government can ensure that the conditions for self-regulation (such as sufficient enforcement) are met. Government intervention is called for where fundamental moral values are at stake, notably fundamental citizen rights and the prevention and investigation of serious breaches of the rule of law and national security. The government should expressly choose between instruments of action: self-regulation, leaving issues for the courts to decide, administrative measures, and formal legislation. [25880, nrs 1-2, 12-14]

The *Electronic Commerce Action Plan* of March 1998 [EZ] is one of the new policy initiatives emerging from the reassessment of the National Action Plan. Noting that the Netherlands has a good potential basis for becoming one of the leading countries in e-commerce, it aims at addressing the barriers that obstruct e-commerce. Among these barriers are legal uncertainties, and the Action Plan consequently sets the government the target of ensuring a clear and coherent legal framework. Moreover, the government should enhance trust and security in electronic transactions. Thus, a national Trusted Third Parties (TTP) project aims at stimulating the development of a reliable TTP infrastructure, which will facilitate and build trust in electronic commerce [KPMG 98].

In all, many countries have taken steps to anticipate the advent of a global information infrastructure (GII). One noteworthy aspect of these steps is that they are being shaped by the interaction of public and private sectors: all actors in the information society are defending their interests in policy debates that often have to build consensus out of conflicting interests. Government-business fora are increasingly being held in this policy-making process.

Not only Western countries, but also countries in Asia, Latin America, and Eastern Europe have recognized the importance of ICT for their economic growth and development. At a GII meeting in July 1994, chairman Brown of the US IITF envisaged the GII "as a web of interconnected local, national and regional networks that would 'substantially further economic growth and job creation, infrastructure improvements, and broad based social discourse within and between and among all countries.'" [quoted in Saxby, 228]

### 2.1.3. Building blocks and participants

The backbone of the information society is the information infrastructure. It consists of several networks and services with providers and users – all interrelated and interconnected. To see how the information infrastructure is built up, one should distinguish between information production and use (which are content-sensitive) on the one hand, and information transport (which is content-neutral) on the other. Again, one can divide the facilities serving information transport into transport networks and transport services. The information infrastructure can thus be modeled as in figure 2.1.



Figure 2.1. *The layer model of the information infrastructure [based on Smits and on Arnbak]*

The infrastructure providers (also called network operators or network providers) operate the infrastructure: telephone, cable, and the electromagnetic spectrum. They provide capacity to the network service providers, or sometimes directly to end users (as with rental lines, which can, for instance, be used for intranets<sup>6</sup>). Networks can be interconnected – for example, phone calls on the GSM system for mobile communications run partly across the ether and partly across the terrestrial telephone network.<sup>7</sup>

---

6 Intranets are a quickly developing market for companies desiring a private network for internal communications. Their functioning and use are often similar to the Internet, but they are not connected to wider, external networks (except, perhaps, through a firewall). A recent development is the restricted opening of intranets to third parties, effectively making the intranet an 'extranet'.

7 Analogous mobile networks (such as ATF and NMT) are quickly yielding ground to digital networks, the most important of which are GSM and DCS-1800. A standard for a Universal Mobile Telecommunications System (UMTS) is being developed, which will incorporate Internet access and video-conferencing services. Besides mobile communications through the ether and the terrestrial networks, satellite personal communications are also gaining ground.

Network services are the basic services that open up the infrastructure to users. They route information from information providers to end users, using the capacity of one or more infrastructural networks. Basic network services are voice telephony (both mobile and stationary), data transport, and radio and television distribution.

On top of these basic services are value-added services (VAS). These add a certain value to the basic service – additional facilities, user interfaces, access to data bases, et cetera. Well-known VAS are the dial-800-services, directory services, e-mail services, Internet access-provider services, data casting,<sup>8</sup> and caller-ID.

The data and information that are transported through these layers come from content providers – artists, program makers, data-base makers, enthusiastic WWW users, and the like. Sometimes, this information is managed through information services that mediate between the makers and the consumers of the information – broadcast companies, electronic publishers, information brokers, or data-base managers.

Figure 2.1 also indicates connections that have just been or will shortly be realized. For instance, cable network providers offer voice telephony services,<sup>9</sup> and ether network providers can offer data transmission services through mobile data terminals. So, the traditional borders between the various networks are disappearing. As the traditional distinction between voice, sound, and text is blurring through digitization and multimedia, the core terrestrial networks of telephone lines and TV cable as well as the air networks of satellite and radiographic transmissions can – depending on their bandwidth – all transport various kinds of data, be they voice, sound, text, or image.

From this model, one can see that the participants in the information society are providers (of networks, services, and content) and users. A third participant is the government, which plays a role not only as an end user but also as a regulator.

#### 2.1.4. Problems

All participants have something to gain in the information society. Providers have great commercial opportunities for new services and for marketing. End users profit from a wide range of interesting and useful applications tailored to their needs. For the government, the information infrastructure offers new opportunities, for instance, raising the general education level, better involving the public in its governing, and opening up its public information through an easily accessible and cheap medium.<sup>10</sup>

However, the information infrastructure is not a *deus ex machina* that provides instant happiness for all. Several problems inhibit the full realization of the opportunities it offers.

---

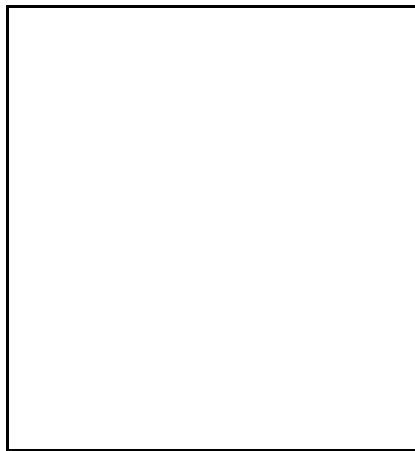
8 Data casting is the process of sending data to a specified group of users along with radio or television transmissions.

9 In April 1996, cable provider Edon started offering telecommunications services in the north and east of the Netherlands via its cable infrastructure. The largest cable network operator in the Netherlands, Casema, is offering telephony via the cable since 1997.

10 Some governments may also use it as yet another medium for propaganda. For instance, the China Internet News Centre launched a video documentary on the Internet <www.China.or.cn>, “which exposes the true colour of the 14<sup>th</sup> Dalai Lama (...) engaged in activities directed at splitting China.” [*China Daily*, 29 October 1997]

I mention some of the challenges the information society faces, in particular those that are directly or indirectly related to the crypto problem.

Network providers face a hard task of interconnecting the several backbones that lie spread across the world. Interconnection and interoperability are primary conditions for establishing an infrastructure that is suited to the needs of the global information society. Yet the disparity of national infrastructures as well as the incompatibility of some of the technologies used hamper the interconnection of all networks into one global information infrastructure.



A second concern is intellectual-property rights. Current legislation is based on traditional media and is widely believed to be inadequate for protecting intellectual-property rights in the information age. The present protection is felt to be interpreted too broadly (particularly by the European Commission) to cover situations in electronic media for which it is not appropriate, whereas the enforcement of intellectual-property law in electronic surroundings is insufficient. These problems have to be addressed, if the still increasing demand for online entertainment as well as for online cultural and educational information is to be met.<sup>11</sup>

A third major problem is the keeping in order of the information infrastructure. Governments on the one hand are liberalizing the telecommunications market, presuming that market competition will enhance technologies and reduce costs for customers. On the other hand, they see the advent of a new medium, perhaps of a new society, in which they have to safeguard at least the basic citizens rights and duties that pertain to the present society. As a medium built bottom-up and belonging to its users, electronic highways can hardly be regulated, but as they are taking over parts of traditional life, governments' desire to somehow regulate them is becoming more compelling. Besides, jurisdiction presents great problems, as the information infrastructure is essentially an international undertaking which does not tolerate nationally-based rules.

Finally, the users of the information infrastructure do not really jump at the potential the providers so alluringly offer them. Two of their main concerns, privacy and security, are insufficiently safeguarded.<sup>12</sup> As long as consumers are diffident that their privacy is being

---

11 The value of intellectual-property rights-related products in the Netherlands was estimated at twenty billion guilders (USD 10 billion) in 1994, according to the National Action Plan [23900, nr 20, 2.2]. The European Parliament is "concerned that the total availability of knowledge, or of the products of the creative process which the term information society conjures up, risks being an illusion if intellectual property rights as a whole are not guaranteed, particularly artists' rights, at the same time as the rights of access and use at reasonable cost for individuals" [*European Parliament Resolution*, 30 November 1994]. See also the third principle of the [NIIAC] document.

12 According to GVVU's 8<sup>th</sup> WWW User Survey, Internet users consider privacy the number one most important issue facing the Internet; for European respondents, privacy is the third most important issue, after navigation and censorship. Although electronic commerce is taking off, "security remains the number one reason Web

### The Internet

The Internet, the mother of all networks, is a network that connects all kinds of networks worldwide. Over 100 million users are guesstimated to have access to its treasures. Most of them are located in North America (around 60 per cent) and Europe (around 20 per cent).

The Internet comprises tens of thousands of mailing lists, which forward e-mail messages to subscribers, and the World Wide Web (WWW), a graphic interface that allows people to create and read homepages with attractive graphics, sound bites, and video fragments. Besides, Usenet serves over 25,000 globally available news groups: gigantic notice boards where everyone can post and respond to messages. FTP (file transfer protocol) services allow people to download documents, and with Telnet, people can login remotely on open servers.

To pin down the significance of the Internet, people have coined many metaphors. Each metaphor emphasizes some aspects, but none covers it satisfactorily. The 'information superhighway' stresses the technological potential of the Internet (opening up the hinterland to new technologies) but fails to incorporate its variety of users and applications (and is somewhat misleading as to the speed of information transfer). The (world wide) 'web' catches the structure of a network with many interconnected nodes, but lacks an innovative sound. The 'never-ending worldwide conversation' and 'a kind of chaos' (as US judge Dalzell worded it) fail to catch the many forms of offering information and the increase in commercial applications. Perhaps the most attractive simile is the Internet as a 'community' – a separate society with its own people and its own values, habits, and culture. It suggests, however, that the Internet is somehow 'disconnected' from the rest of the world: a distinction between 'the Internet' and 'the real world' that is misleading if anything. The Internet, after all, is as real as television, school, or the pub.

The volatile, ungraspable character of the Internet is caused by its variety of manifestations, its ever changing and diverse population, and its focus on technical rather than legal regulation. Started in the 1960s as the ARPAnet, a research network with defensive components, the Internet has gradually evolved into an international network linking universities, government institutions, businesses, and individuals, only to fully emerge in the 1990s as the prime banner-bearer of the information society. Especially since the advent of the WWW, its growth has been exponential, the end of which is not yet near.

The Internet was built up by its users and is said to belong to its users. They will not hear of control or regulation; their own 'rules' – or lack thereof – are sufficient to keep everything in order. Netiquette, the do's and don'ts of Internet communications, is the main set of rules to take into account. This self-regulation works, the Internetters say. Governments increasingly disagree and – with visions of the four horsemen of terrorists, child pornographers, drug dealers, and money launderers – argue that some control is inevitable. But how do you control a web-like virtual supercommunity?

threatened by the unlimited collection of personal data, they will be reluctant to engage widely in electronic transactions. Moreover, generally accepted and secure systems for electronic payment are required before electronic commerce can really take off.

These problems have to be addressed before a global information infrastructure can really emerge. That it *will* emerge in the end, few people doubt, but just *how* it will take shape depends on the solutions that will be chosen to address the problems.<sup>13</sup>

---

users report for not purchasing over the Web". [GVU] A report by INRA (Europe) of January 1997 polled the EU member states; they found that two thirds of the respondents worry about leaving tracks of personal information on information networks by using them. [INRA] "Without the legal security of a Union-wide approach, lack of consumer confidence will certainly undermine rapid development of the information society. (...) INTERNET is so big, and growing so fast, that it cannot be ignored. Nevertheless, it has its flaws, notably serious security problems." [Bangemann 94, 18-23]

13 The hopeful visions of future benefits of a global information infrastructure can become reality, but it may take a generation or so to take full effect. As a sensible report of the International Telecommunication Union words it: "Our children are the ones that will really benefit from the global information infrastructure." [quoted in *CLSR*, March-April 1996]

## 2.2. Information security

In the information society, information is of primary importance. People and enterprises are increasingly growing dependent on information. The protection of information from loss, unauthorized altering, or disclosure is therefore a major concern. According to the EU *Green Book on the Security of Information Systems*, “2/3 of the economy (...) depends critically on the accuracy, security and trustworthiness of information” [DG XIII, section 1].

Several developments have contributed to the growing importance of information security. Where information-processing systems used to be sparse, confined to well-defined, guarded buildings, and so complex that only a few people knew how to handle them, nowadays computers are all-pervasive and often linked over insecure networks, and ever more people know how to operate them.

Businesses attach increasing importance to the reliability of their information-processing systems, not only because the integrity or confidentiality of the information is essential for the company’s manufacturing or services, but also because customers are making more demands on the reliability of the enterprise. With the globalization and deregulation of the economy, competition gets fiercer. A company’s image is crucial to its viability, and computer security-related incidents can be fatal as the public loses confidence in the company’s reliability. Moreover, industrial espionage is a major concern for larger enterprises who depend on the secrecy of their manufacturing processes, research and development, or contract negotiations.<sup>14</sup>

The advances in computer technology have also contributed to the growing importance of information security. A vast number of new applications and an enormous increase in computing power are causing entire areas of life to be digitized. So, alternatives have to be found for the traditional ways of protecting these areas and of securing privacy.

Most importantly, computers are being interconnected in ever larger networks, not only via the Internet, but also in private networks (intranets and extranets) and Local Area Networks. Where physical control used to suffice to protect single computers stored in guarded buildings, networks need a different kind of protection.

This section deals with information and communications security objectives, threats, and measures, and with the role of governments in facilitating information security. As a case study, I will sketch the (lack of) information security within the Dutch government.

---

14 In 1993, a German consortium led by Siemens lost a major order for a high-speed train in South Korea to the British-French GEC-Alsthom. Information intercepted through the global surveillance system Echelon was thought to have given GEC-Alsthom a crucial advantage. In January 1994, French Airbus lost a six-billion-dollar order in Saudi Arabia to Boeing and McDonnell Douglas, because Clinton had offered to meet the constraints that king Fahd had asked the French for in vain; American security agents boasted afterwards they had won the order through their interception capabilities. Also in 1994, US Raytheon outsmarted French competition in a Brazilian radar order. The fact that Raytheon met the Brazilian demands in all respects just a little better than the French inevitably suggested they had used signals intelligence. [Brouwer] In mid-1996, the US intelligence service was rumored to have hacked into the computers of the European Parliament and the European Commission in order to obtain economic information. [ *Sunday Times*, August 1996]

### 2.2.1. Objectives

The three basic objectives of information security are confidentiality, integrity, and availability: the CIA of information security. An additional objective is non-repudiation.

*Confidentiality* is the requirement that information is kept secret from people who are not authorized to access it. In communications security, it can include the requirement that traffic analysis be prevented, that is, that information about who communicates with whom when, how often, and from where is kept secret. Confidentiality is sometimes referred to as exclusiveness.

*Integrity* is the requirement that information is unaltered and complete, or, in the ITSEC definition, that information “is modified only by those users who have the right to do so.” [ITSEC] A similar requirement, sometimes understood as a part of integrity, is *authenticity*, the certainty that the message indeed originates from the purported sender. In practice, these two objectives are closely interrelated: safeguarding authenticity usually implies safeguarding integrity (and often vice versa). I shall handle integrity and authenticity as distinct but related objectives.

*Availability* is the requirement that information and information and communications systems are available to their users at the right time.

*Non-repudiation* means that the sender or receiver of a message cannot deny having sent or received the message. This is particularly important in situations where sending or receiving a document constitutes a legal act. For instance, in business transactions, it can be essential to invoke liability rules, and in sending electronic appeals to a court, it can constitute the difference between conviction and acquittal.

### 2.2.2. Threats

Information and information systems are threatened from all sides. Natural disasters, such as earthquakes or floods can destroy information facilities as well as (backup) information. Animals like (kamikaze) squirrels or raccoons electrocute themselves in power generators, putting down entire systems for days [Neumann, 85].

People threaten information in a variety of ways. *Unintentional* incidents, such as password loss, infecting the corporate system with a home-copied virus, or spilling coffee over a keyboard are typical examples. A widespread security flaw is weak password protection. Many people choose easily guessable passwords, and others are careless with their passwords.<sup>15</sup> A study estimates that 80 per cent of security-related incidents in the Internet have to do with improper use of access codes and passwords [Fraser]. Many of these are made possible by the neglect of authorized users – or they are perpetrated by them.

---

15 Former French president Mitterand, on his first day in office, put the paper with the code for launching the atomic weapon in a suit pocket (contrary to Pompidou and Giscard, who wore it engraved in a necklace). He forgot all about it, and the code was only saved just before the suit was brought to the dry cleaner's. [Volkskrant, 18 May 1995]

Although it does not necessarily cause more damage than carelessness, *intentional* computer misuse has received by far the most attention.<sup>16</sup> Especially external threats from hackers and virus producers are notorious.

Hackers can cause extreme (real or symbolic) damage, such as the Dutch hackers who retrieved hundreds of US military secrets which they offered to Saddam Hussein during the Gulf war.<sup>17</sup> They are by definition hard to trace, and likely a great number of hacks remain undiscovered. Still, as computer-security expert William Cheswick has noted, “the fact that so many security holes have gone unused for so long could mean that there are far fewer malicious hackers on the Internet than the din of dire public pronouncements would have people think” [Wallich].

Over 10,000 viruses roam computer networks and personal computers to do their malicious (or sometimes beneficent) jobs. Anti-virus software protects against the bulk of known viruses, but new viruses appear all the time – an estimated six a day [Kephart]. Most recently, the new family of macro viruses appeared on the stage: small programs which automatically execute some action in a word-processing or spreadsheet program. Macro viruses spread from document to document, and so, they travel frequently as attachments to e-mail messages.<sup>18</sup> Some viruses are resistant against most anti-virus software by masquerading or transforming themselves proteanly every time they copy themselves onto another system (some use cryptography to do this). Viruses remain a serious threat and are more pervasive than hackers.

Despite the publicity given to intentional break-ins from the outside, the vast majority (an estimated 80 per cent) of computer security-related incidents are caused by internal users [Wright 95].<sup>19</sup> Studies of computer-related crime regularly find that a high percentage of the perpetrators are employees who have regular access to corporate information and information

#### Political viruses

Viruses can have political implications. A virus spread around China in the early 1990s asked the computer user whether Li Peng was a good prime minister. If you answered no, the virus did nothing, but if you affirmed the leadership qualities of Li Peng, the virus erased the entire hard disk. [Kristof, 279] The Dutch green-left party GroenLinks considered launching a virus in a voting campaign. The virus would pop up a slogan inciting to vote for GroenLinks. In the end, the party decided not to spread it – perhaps unfortunately, as the virus would have immunized computers against the much more harmful Jerusalem virus [Sophos, 135].

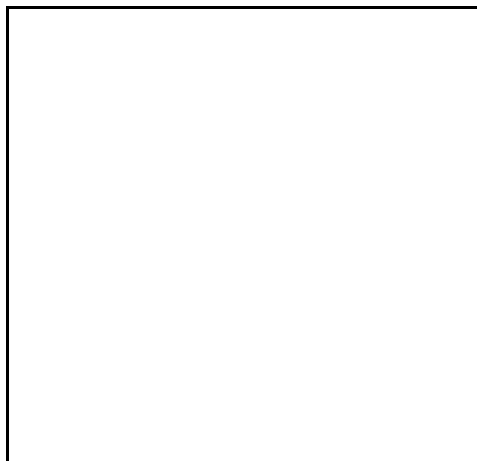
US government intelligence experts (the Moynihan Commission) showed their ignorance in a report on protecting government secrecy, when they warned against the virus Penpal Greetings “that could infect the hard drive and destroy all data present”. [*Crypt newsletter*, April-May 1997] In reality, Penpal Greetings is a hoax virus: a message continually being sent around the Internet that warns against a non-existent virus. Penpal is a little brother of the notorious GoodTimes ‘virus’.

16 Although most of these threats attack the confidentiality or integrity, some attacks harm the availability of ICT. For instance, stealing communications lines can “seriously disrupt the national system” (in the words of the Chinese *Legal Daily*) – but executing nineteen people for this seems somewhat out of proportion, even by Chinese standards [*The Independent*, 17 July 1996].

17 According to intelligence experts, this could have potentially changed the course of the war, had not the data been ignored by Iraq – probably because they feared a hoax. [Reid]

18 “Since the first macro virus appeared in the wild in July 1995, the speed of its spread and the scale of infections have probably surprised even the gloomiest doom merchant.” [Hruska]

19 “Survey after survey over the past years has shown that the greatest threat to computers is to be found not from the sophisticated attack perpetrated by a highly motivated outsider, but from the simple error, omission, or malicious action of an employee.” [Smith, 418]



systems. Notably computer fraud, data diddling, and placing logic bombs are popular with them. Well-known cases of computer fraud include a Rotterdam municipal official who embezzled six million guilders (at the time about USD 3 million) by adding pay orders to the daily pay file after the automated check-up had taken place. Several cases are known of disgruntled employees who placed logic bombs in the corporate system to destroy key information or block all access, for ransom or out of spite.<sup>20</sup>

The number and variety of threats to information security are growing along with computer technology [Neumann, 168].<sup>21</sup> Since

security technologies are also advancing, threats and protection remain more or less balanced, and so, the general level of security threats remains roughly the same [Neumann, 178].

### 2.2.3. Measures

The implementation of an information-security policy varies with the situation. No single security measure provides full security (if 'full security' exists at all), and so, a combination of physical, technological, and organizational measures may be called for to achieve the desired level of security.

*Physical* security measures, such as isolating key information and vital information systems in closely guarded rooms, are important, but they can be impractical. *Technical* measures include hardware and software protection of networks and of data themselves. With a connection to a larger network, such as the Internet, a firewall can shield a local network from intrusions.<sup>22</sup> Cryptography is the main way to shield information itself. *Procedural* measures, such as responsibility division or the regular changing of passwords, are necessary to back up the physical and technical measures. *Inspection and auditing* have to assure

---

20 For instance, after his dismissal, an employee of Omega Engineering Inc. allegedly activated a computer 'bomb' which permanently wiped out the company's critical design and production programs, causing an alleged loss of USD 10 million. [ECLR, 25 February 1998]

21 The *Code of Practise for Information Security Management* voices the expectation that the threats to information security will continue to increase and grow ever more serious and refined. [BSI]

22 Even firewalls do not provide complete protection (see Ch. 3, note 45). The computer language Java allows small applications (applets) to be downloaded to run on the downloader's system. This can undermine the firewall's protection against outside threats. "If a Java program can access users' files to help bring order to their electronic life, it can also easily wreak disorder (...) and bring the Net to its collective knees. (...) In theory, strict cryptographic safeguards should prevent mischief, but the system has yet to be thoroughly tested." [Steven Cheswick, quoted in Wallich]

detection and tracing of security violations; they can be regarded as the final piece of an information-security policy.<sup>23</sup>

Security measures, however, can severely limit the convenience of information processes. In general, a trade-off has to be struck between security, ease of use, and costs. Because information security costs money without yielding obvious gains, it is not evident to give it wide attention, and businesses and institutions may fail to fully realize the importance of the confidentiality, integrity, and availability of their information.

#### Information-security policy

Given the variety of threats information is exposed to, and the fact that security objectives vary with each situation, no general rules can be given for implementing information security. Each enterprise or institution has to make its own policy, based on an internal risk analysis that takes into account the particular circumstances of the environment.

The risk analysis has to include an analysis of possible security incidents, the damages these might cause, and an estimate of the likelihood that such incidents occur. It is vital that all aspects of information security are taken into account, because security is only as strong as its weakest link. It is useless to implement secure mechanisms such as encryption or firewalls, if confidential information can be found in the waste-paper basket ('dumpster diving') or if employees can easily be lured with bribery without risking discovery.

An overall policy, therefore, is essential in information security. One of the main theses of the *Code of Practise for Information Security Management* [BSI] is that this policy needs the backing of the management in order to assure that all measures are followed in practice. Only an integral policy can effect the level of security called for.

#### 2.2.4. Governments' role in information security

The importance of information security has been recognized in several government initiatives and reports. The 1992 OECD *Guidelines for the security of information systems* provides a framework for private and public bodies to implement a consistent and adequate program for protecting their information systems.

In 1992, the European Council adopted a *Council decision in the field of the security of information systems* [92/242/EEC], which comprised the development of overall strategies for information security (an action plan), and the setting up of a Senior Officials Group (SOG-IS) to advise the Commission. As an intermediate step to formulating the Action Plan, in October 1993, the Commission published a *Green Book on the Security of Information Systems* (the draft of which was never officially adopted) [DG XIII]. The INFOSEC program has subsequently been investigating several policy areas in information security, most recently within the framework of the European Trusted Services (ETS) framework [ETS].

The 1997 EC Communication *Ensuring security and trust in electronic commerce* provides a policy framework for information security, focusing on integrity and authentication services (digital signatures) and confidentiality services (encryption). This should lead to, among others, a European framework for digital (or, broader, electronic) signatures [COM(98) 297], and the integration of cryptography within the framework of other European policies, such as privacy protection and intellectual-property rights.

---

23 The *Computer Security Handbook* lists as minimum requirements for communications and network security: employee awareness and vigilance, password and access supervision, hard-copy control, encryption, and frequent log monitoring [Hutt, 17.21].

In the United States, the (sadly deceased) Office of Technology Assessment published *Information Security and Privacy in Network Environments* [OTA]. This study addressed policy issues in the areas of cryptography policy, safeguarding unclassified information in federal agencies, and legal issues and information security, including electronic commerce, privacy, and intellectual property. The NII Security Issues Forum released a draft report *NII Security: The Federal Role* [NIISIF], calling for a government role in supporting a secure NII by facilitating private-sector activity, ensuring public safety by protecting against abuses, and supporting research and development. It stressed, however, that much of the responsibility lies with the private sector. Security is also one of the issues in the *Framework For Global Electronic Commerce*. For a secure GII, a range of technologies, supported by trustworthy infrastructures, are required, and the US government, in partnership with industry, is taking steps to promote such technologies [Clinton, 20-21].

All of these documents stress the importance of information security – it is a vital issue in the present information society. With the increasing importance of information and information-processing systems, protecting the confidentiality, integrity, and availability of information needs full attention.<sup>24</sup> Governments should ensure that measures to enhance information security are developed and that their use is stimulated, while there is a primary role for the private sector to see to the shaping and implementation of these measures.

### 2.2.5. Information security in Dutch government

Considering their information-security policy documents and regulations, one expects governments to be careful with information protection. They handle sensitive, privacy-related, and confidential information. However, significant parts of the Dutch administration seem to be rather unmindful of information security.

For instance, the justice department of The Hague district discarded computers, selling them to a Nijmegen company. A student in Nijmegen bought one of them, and found confidential information – psychiatric reports, interrogation reports, correspondence – from judges, prosecution officers, and court clerks. She forwarded it to the regional newspaper. [ANP, 8 December 1995] A new system was installed at the Central Criminal Intelligence Agency in The Hague; shortly afterwards, “[c]riminals were set free, and innocent people were arrested. The computer system was taken out of service. Unfortunately, the back-up system had been decommissioned. The vendor blamed the police for using the system incorrectly.” [Neumann, 175-176] The police in Southern Limburg lost documents on contentious investigation practices, due to a convenient computer crash [De Limburger, 3 November 1997].<sup>25</sup>

More importantly, law-enforcement agencies increasingly face counter-strategies by criminals attacking their information resources. In August 1994, prosecution officer Valente had taken home some fifty diskettes with investigation and prosecution information. The

---

24 “There is an urgent need to address requirements and options for action in the field of security of information systems at national, Community and international level in close collaboration with sector actors and national governments. Any action must take into account both national and international commercial, legal and technical developments.” [DG XIII, section 1]

25 Losing important files is not only caused by computer incidents. A theft case stranded at the Dutch Supreme Court because the “documents had been lost” [HR 29 October 1996, nr 103.446].

### Information security in EU and Dutch law

In some situations, information security is mandatory. Many countries have data-protection laws which require processors of personal data to adequately protect the data from unauthorized access or altering. The 1995 European *Directive on the protection of privacy with regard to the processing of personal data and on the free movement of such data* states that "the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." [95/46/EC, art. 17a para. 1]

In addition to this general Data Protection Directive, the *Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector* requires that the "provider of a publicly available telecommunications service (...) take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented." [97/66/EC, art. 4]

The Dutch Data Registries Act requires holders of personal data registries to take "the necessary technical and organizational measures to protect a personal registry against loss of or damage to the data and unauthorized cognizance, alteration or supply thereof" (art. 8). Following the EU Data Protection Directive, the Data Registries Act is to be replaced by a new Data Protection Act. Article 13 of this draft DPA requires proper technical and organizational measures to protect against loss or any kind of unauthorized processing of personal data. The measures should guarantee an adequate level of protection, taking into account the state of the art of technology, costs, the risks, and the kind of data involved. The Police Registries Act of 21 June 1990 has a similar requirement as the Data Registries Act on the security of police registries. According to the Dutch Act on Municipal Basic Registries of 1 October 1994, the State is responsible for assuring the security of the network of municipal basic registries; the protection of the registries themselves will be regulated by implementing order. Possibly, municipalities will be required to encrypt their registries [Schönfeld, 24].

In the Netherlands, hacking is punishable only if security measures have been infringed (art. 138a DCC). This serves as an injunction to computer users to take security measures. In 1993, the Dutch Civil Code was expanded with an obligation of the accountant to include in his report to the board of commissioners his findings on the reliability and the continuity of the company's automated data processing (art. 2:393, para. 4).

Information security in departments is the subject of several guidelines, such as the *Decree on government-department information-security instructions 1994*. The *Governments Accounts Act* charges the departmental accountant with the care for information security.

diskettes were stolen, and the unprotected information was leaked to the press, causing significant embarrassment. [Traa, 187] After a burglary at two police agents' homes in Almere, information on a murder case from stolen diskettes was published by a tabloid [*Volkskrant*, 1 June 1996]. A businessman from Amersfoort claimed having bought his police file for USD 200 – within an hour, someone had cracked the police computer system for him and delivered the file on diskette, with the codes for decoding and all [*Volkskrant*, 16 June 1995]. Thieves entering the Zeist office of the National Police Services Force in December 1996 stole some portable computers; the suitcase containing the portable computers also contained a handwritten note with the access codes [25208, nr 1].

Also, communications among law-enforcement agents are regularly being monitored.<sup>26</sup> The same criminal organization that stole diskettes at Valente's home was suspected of recording his telephone conversations [Traa, 187]. Indeed, many cases were reported of scanner-freaks who were constantly locating police teams; they eavesdropped on telephone lines and walkie-talkies, for example, of Valente and police officer Woelders [Traa, 67]. Even despite being encrypted, mobile-phone conversations were sometimes recorded and cracked:

<sup>26</sup> Warrington police agents were fed up with their mobile phones being monitored. They reported over the police radio that a UFO had crashed on a nearby field, and told how to reach that field. Within minutes, people came nosing around – to be arrested on the spot. [*London Times*, 23 March 1994]

the Amsterdam police found tapes during a search with the decryption of encoded conversations [*Volkskrant*, 3 May 1996].

Following such incidents, security measures have been taken. The Minister of Justice in 1993 confirmed that to protect police radio conversations from being monitored, “indeed a larger spread of encryption equipment was intended.” [23047, nr 12, 1] The Valente incidents led the Public Prosecutor in 1994 to order better protection for courts and sensitive information [OM94]. In 1996, the Brabant-Zuidoost police adopted a secure crypto system for their radio communications [*ANP*, 21 March 1996]. The Van Traa committee accorded addressing the threat of counter-strategies a high priority in order to prevent these activities from influencing the maintenance of law and order [Traa, 71]. Consequently, in April 1997, a *Police Information Security Regulation* took effect, requiring police-force managers to implement information-security policies.

Other parts of government also handle sensitive information, but security policies are sometimes lacking. For instance, the Chamber of Audit found that the information security within the Dutch Internal Revenue Service, although improved, was still seriously flawed in 1997. The access to its automated systems was not adequately protected. For example, officials were careless with their passwords, and too many people had access to confidential information. [25290, nrs 1-2] Municipalities have widely varying information security policies – if they have one at all. A 1996 study concluded that only 30 per cent of Dutch municipalities have a worked-out security plan. Only 20 per cent conform to the data-protection guidelines of the Data Protection Authority. Of the municipalities connected to the Internet, 63 per cent had not taken additional security measures. In 1997, the municipal audit department of Amsterdam found that the security of computer registries of personal data was functioning badly, making municipal services vulnerable to fraud and corruption [*Het Parool*, 15 October 1997]. The Chamber of Audit found in 1995 that of all Dutch ministries, only four had an adequate policy on information security. The central authorities still ran risks of loss, unintentional disclosure, and unauthorized alteration of data, and the ministries themselves had insufficient understanding of the scope of these risks [24175, nrs 1-2]. With the *Decree on government-department information-security instructions 1994* that came into force in January 1995, one may hope the departments are now better implementing information-security policies.

The lack of good information-security measures in government is all the more pressing, as more and more areas of the administration are being digitized and interconnected. For instance, the ‘Government Office 2000’ initiative plans to offer a one-stop-shop service for citizens: they can access all relevant government information from a single, public terminal. This calls for the highest security level, as interconnecting all kinds of data bases renders the system extremely vulnerable.

### 2.3. Conclusion

The information society is in the making. Information and communications technologies are shaping the information infrastructures, and all parties involved – providers, users, and the government – have a lot to gain. The establishment of the information society is for a large part the task of private investors, while governments focus on stimulating the development of a national (and global) information infrastructure, providing a motivating and balanced regulatory environment, and giving citizens transparent access to government information.

Governments must address several problems which currently inhibit the information society from fully developing. One of these problems is information security, a major interest in the information society. “Democratic societies engaged in the global economy need to provide for appropriate levels of information security.” [SOG-IS]<sup>27</sup> Governments have recognized the importance of information security: although it is up to the private sector to establish adequate security measures, governments are committed to stimulating the development and putting into practice of good security policies. The fact that information security is not yet fully incorporated into all sectors of government, as security breaches within the Dutch government show, indicates that governments should also safeguard the implementation of adequate security measures for themselves.

---

27 In a way, the need for information security can be compared to the public need of traffic safety: “Establishing security for information and communications technologies can be regarded as a society task in line with the treatment of traffic safety on the public roads.” [Stripp, 60]