

## European Initiatives on Network and Information Security

a report by

**Frans de Bruïne**

*Director, DG Information Society, European Commission*

Frans de Bruïne is Director of the DG Information Society of the European Commission. He is responsible for communications and network technologies, networked audiovisual systems and home platforms, software technologies and distributed systems, trust and security and e-business. In addition, Mr de Bruïne is responsible for the eTEN programme (formerly TEN-Telecom), which stimulates the development and deployment of networked services in Europe. Between 1975 and 1990, he worked within the Ministry of Economic Affairs as Section Head of New Energy Sources, Deputy Director for Research and Development, Director for Technology Policy and Managing Director of the Dutch Technology Agency. Mr de Bruïne has a Masters in Physics from the Technological University of Delft and a Bachelors in Economics from Erasmus University, the Netherlands, and he participated in an Advanced Management Programme at the Institut Européen d'Administration des Affaires (INSEAD), France.

### The Advent of the Information Society and the Need for Enhanced Network and Information Security

The vision of an information society goes back to the white paper by Jacques Delors: "Growth, competitiveness and employment: The challenges and ways forward into the 21st century" in 1993. Since then, the world has gone through a number of technology-led transformations and business cycles that have contributed to clarifying the economical and societal potential, opportunities and challenges of this vision. It is against this background that, in March 2000, the European Council adopted the so-called Lisbon Strategy that set the goal for the EU to become the largest and most competitive and dynamic knowledge-based economy by 2010.

Attaining this goal would only be possible by networking and embedding more and more advanced information and communication technologies (ICT) in innovative systems and services critical for business and daily life. Such developments are envisioned in the ambient intelligence space that anticipates how advanced technologies would enable and support completely novel scenarios of shared computing and networking resources and capabilities featured by ubiquity and mobility. However, such developments would only be possible with innovative, enhanced and more transparent security.

### Security in the Ambient Intelligent Space

Rarely in history have we faced the challenges – or the remarkable opportunities for progress – that we face today. It is reasonable to say that breathtaking advances in ICT are taking place at astonishing speed. In addition, in Europe rarely, perhaps, have we had in our hands the knowledge, the cultural heritage and the political momentum to meet both these challenges and opportunities.

The personal computer is gradually becoming less central to our lives, with novel and smaller devices and equipment becoming more and more pervasive. Our personal environments are increasingly

populated with smart mobile phones, hand-held info-appliances, personal networks and computer chips plugged everywhere (in our cars, in our homes and even our clothes).

The on-going convergence of information, communication and media technologies and industries drives a shift of paradigm from ICT to ambient intelligence, by which people are empowered through a digital environment that is aware of their presence and context and is sensitive, adaptive and responsive to their needs, habits, gestures and emotions. Such ambient intelligent environments will feature ubiquity (i.e. people are surrounded by a multitude of interconnected embedded systems that are invisible and moved into the background of our environment), awareness (i.e. the ability of the system to locate and recognise objects and people and their intentions), intelligence (i.e. the digital surrounding is able to analyse its context, adapt itself to the people who live in it, learn from their behaviour and eventually understand emotions) and natural interaction (i.e. natural speech and gesture recognition, as well as speech synthesis, which will allow a true user-friendly communication with the digital environment).

In the ambient intelligent space, people will participate in a multiplicity of parallel, overlapping, interleaved and evolving one-to-one, one-to-many and many-to-many relationships, some of which will be short-lived, and some of them established temporarily and instantaneously. The human-machine relationship will no longer be explicit but will actually be implicit: one's everyday surroundings are to become the interface.

Europe has been a pioneer in the development of the ambient intelligence concept. As early as 1999, the IST Advisory Group (ISTAG), which provides the European Commission with independent advice concerning the direction and content of research work in the field of ICT, declared the vision to "start creating an ambient intelligence landscape for seamless delivery of services and applications in Europe relying also upon testbeds and open source software, develop user-friendliness, and develop and converge the networking infrastructure in Europe to world-class."

# STORAGE NEEDS MULTIPLYING TOO FAST?



**TAKE CONTROL WITH**  
**magnitude** 

Manage More With Less.

Quit hopping from one storage crisis to another. Simplify your data management with the XIOtech Magnitude™ storage solution. It's the only solution that simplifies storage *and* server management, allowing your IT staff to perform complex tasks in seconds—on the fly, as demand dictates. Now you can easily control growing storage requirements and keep a handle on your costs at the same time. It's the Magnitude difference.

Request your **FREE** Magnitude information kit by calling 1-866-472-6764 (+1 952-983-3000) or visit us at [www.xiotech.com](http://www.xiotech.com).

Because of certain major trends, such as the growing number of subjects and objects moving constantly in ambient networks, the heterogeneity of systems and infrastructures, the complexity of both hardware and software and the scattering of knowledge, security will require solutions that are very different from those of today's systems. We are at the beginning of a change in how network and information security is approached; in fact, more is to change in security than in any other issue.

For a world with ambient intelligence, we need ambient security. Security in the ambient intelligent space is a new frontier. It will possess revisited dimensions: ethics, adaptability, dependability and resilience. It will also require a new nature: mobility.

The important question is how Europe will prepare itself for playing a leading role in trust and security in the ambient intelligent space.

#### **Towards a New Paradigm for Network and Information Security**

The more networks and information systems become an essential part of business and daily life – and therefore of the smooth development of the global information society – the more security becomes a necessity. For many generations, people have protected their assets and their privacy using account books, fences, locks, meters, seals and signatures. As civilisation has been progressing, these have been supported by a host of social constructs, ranging from international treaties through national laws to manners and customs.

This remains true indeed. The security perspective in the digital age is about protection of consumer rights (e-confidence), protection against cyber abuse (profiling, fraud and identity theft) and protection of the information infrastructure (intrusions and attacks). The growing awareness of the need for network and information security is being driven by the widespread abuse of the Internet for hacking, virus propagation, 'spam' e-mails, spoofs, denial-of-service attacks and so on. Besides its huge potential for economic growth, industrial competitiveness, employment and social welfare, the advent of the information society is reshaping the risks and nature of possible attacks. 'Old crimes' and criminals are changing the pattern of their operations by using modern technology, whereas new crimes exploit modern technology and attacks against the information systems and technical infrastructure are spreading. Therefore, an appropriate mix of protective measures – technological, organisational and regulatory – should be developed and applied on the basis of those already existing.

Network and information security should be regarded as being a collection of hardware, software,

services, procedures and policies designed to:

- protect an organisation or individual's ICT assets;
- detect and prevent attacks by criminals and terrorists against the information systems and network infrastructures; and
- deter criminal offences that use computers and electronic networks.

At the same time, however, the security environment is changing fast. Most records are now electronic, transactions are increasingly electronic and everyday systems have been automated. By 2010, almost every electronic device that affects our life will be connected to the next-generation Internet. Just as the second half of the past century brought a profound revolution in security engineering due to the development of the underlying technologies (cryptography, software reliability, tamper resistance, security printing and auditing, etc.), the first decade of this new century can be the period of a new paradigm for network and information security. Until recently, security technology has consisted of an archipelago of mutually suspicious islands: the mathematicians working with ciphers, the operating system protection people, the burglar alarm industry and the chemists developing bank-note inks. Such scattering of the expertise or proliferation of particular specialities, added to the fact that security does not yet form an integral part of the design and management of the information system life-cycle, has thwarted most efforts, especially in Europe, to develop a culture of security for all stakeholders. In the years to come, network and information security will be about ensuring that systems are predictably dependable in the face of all sorts of malice and resilient in the face of error and mischance. This means that robustness with respect to human neglect and incompetence will be at least as essential as robustness towards fraudulence. This will lead security managers to pay close attention to economic and institutional issues as well as technical ones, and all stakeholders in general to promote and sustain a culture of security where the traditional 'security islands' will be linked and where industry, users and governments will enter into co-operation and dialogue.

The response to the security challenges posed by the advent of the information society (and the foreseeable development of an underpinning ambient intelligent space) cannot rely only on technical or legal means. Indeed, the complexity and scale of such challenges call for an innovative approach in which policy, regulatory and technological measures would have to be made to work together coherently.