Cybersecurity Guide for Developing Countries

Release 2009

Enlarged edition

Disclaimer

References to specific countries, companies, products, initiatives or guidelines do not in any way imply that ITU endorses or recommends the countries, companies, products, intitiatives and guidelines in question over other similar ones which may not be mentioned.

Opinions expressed in this publication are those of the author and do not engage ITU.

Acknowledgments

This guide, *Cybersecurity Guide for developing countries*, was prepared by professor Solange Ghernaouti-Hélie, (University of Lausanne – Faculty of Business and Economics, Switzerland).

The author would like to thank, for this specific 2009 enlarged edition, Mr. Marco Obiso, ICT Applications and Cybersecurity Advisor, ITU-D and Mr. Igli Tashi, research and teaching assistant from the University of Lausanne.

For the previous editions (2006, 2007), the author would like to thanks Mr Alexander Ntoko, Head of the E-strategies Unit of BDT.

The preparation of this handbook would not have been possible without the excellent cooperation of the members of ITU-D in particular Marco Obiso and previously Alexander Ntoko. We also wish to express our appreciation to ITU Publication Composition Service' team for their work in producing the Cybersecurity Guide.

The *Cybersecurity Guide for Developing Countries* is a project of the ITU Telecommunication Development Sector's ICT Applications and Cybersecurity Division. It is part of a broad range of activities promoting cybersecurity.

The Telecommunication Development Bureau of ITU wishes express its gratitude to professor S. Ghernaouti-Hélie for her contributions towards a more secure and safer information society.

The latest version of the *Cybersecurity Guide for Developing Countries* is available at:

http://www.itu.int/ITU-D/cyb/publications/index.html

For further information on the toolkit, please contact:
ITU-D ICT Applications and Cybersecurity Division (CYB)
Telecommunication Development Sector
International Telecommunication Union
Place des Nations
1211 Geneva 20 - Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Foreword

This cybersecurity guide for developing countries has been prepared for facilitating the exchange of information on best practices, related to cybersecurity issues and to meet the stated goal of the **Global Cybersecuriry Agenda** (GCA) to "enhance security and build confidence in the use of information and communication technologies (ICT)".

The guide is intended to give developing countries a tool allowing them to better understand the economical, political, managerial, technical and legal cybersecurity related issues in the spirit of the Global Cybersecurity Agenda. The purpose of it is to help countries get prepared to face issues linked to ICT deployment, uses, vulnerabilities and misuses.

The content of the guide has been selected to meet the needs of developing and, in particular, least-developed countries, in terms of the use of information and communication technologies for the provision of basic services in different sectors, while remaining committed to developing local potential and increasing awareness among all of the stakeholders.

The guide is not intended as an exhaustive document or report on the subject, but rather as a summary of the principal issues currently encountered in countries wishing to take advantage of the benefits of the information infrastructures in order to build an inclusive information society.

This guide provides them with examples of solutions that other countries have put in place in order to deal with cybersecurity problems. It also refers to other publications giving further, specific information on cybersecurity. In order to avoid any duplication in the treatment of these subjects, the work already accomplished within the framework of ITU-SG, ITU-T, ITU-D and ITU-R were duly taken into account in elaborating the content of this publication, as were the other existing studies and publications in this area.

Summary of contents

The Cybersecurity Guide for Developing Countries is structured in five independent parts that can be read either in sequence or separately.

Part I identifies the context, stakes and challenges of cybersecurity. The purposes of this part are to:

- Indicate some information society considerations and changes implied by the use of information and communication infrastructures;
- Identify the stakes, challenges and issues related to cybersecurity for developing countries;
- Define the main characteristics of cybersecurity; and
- Present the fundamentals of a global cybersecurity approach and the ITU Global Cybersecurity Agenda initiative.

Part II presents cyberthreats, cyberattacks and cybercrime issues in order to be able to answer the following questions:

- What is cybercrime?
- Why and how is cybercrime possible?
- Why is it important for developing countries to overcome cybercrime and cybersecurity issues?
- How could developing countries fight against cybercrime?

A comprehensive approach is proposed to understanding the issue of cyberthreats and cyberattacks, and cybercrime is defined and illustrated to help developing countries get prepared to face the issues and challenges linked to cybercrime and to the deployment of information and communication technologies (ICT).

Part II also presents:

- The basicsof telecommunication networks and Internet technologies in order to understand how cyberthreats can become a reality;
- Sources of vulnerability of the Internet;
- The types, tools and operation of cyberattacks; and
- Examples of misues of ICT and different expressions and examples of computer-related crime and cybercrime. Most cybercrimes are illustrated by real cases of attacks, in order to better understand what cybercrime is. These examples of cybercrime cases, taken mostly from developing countries where the Internet is already widely used and this type of crime is well reported, have been anonymized.

Part III proposes legal, justice and police approaches related to cybersecurity and cybercrime issues. This part demonstrates the fundamental role of forensic computer techniques in cybercrime

investigation and identifies some legal issues related to cybercrime and international cooperation that contribute to preventing, deterring and fighting cybercrime.

The Convention on Cybercrime (Council of Europe) is presented as an example of identifying areas of law to be addressed when dealing with e-activities. In addition, several legal aspects of cybersecurity which contribute to building a safer information society are analyzed. A discussion on privacy issues in the information society concludes part III.

Part IV introduces a technical approach to cybersecurity, presents the most relevant principles of computer security, and specifies the domains of application of cybersecurity. To ensure the availability, integrity, confidentiality, and non-repudiation of resources and services in networked environment, relevant security technologies are explained; some e-mail and e-commerce risks issues are discussed and security solutions given.

The importance of technical security measures to decrease the number and impacts of cyberattacks is presented. The need is identified for a complementary technical, procedural and managerial security approach towards the control and prevention of informational risks, and towards improving the efficiency of security solutions.

The managerial approach of this guide - **Part V** focuses on managing risks and security in a context of business intelligence. It contributes to understanding how to build a cybersecurity strategy, define a cybersecurity policy, and implement security measures.

The objectives of this part are to:

- Define the information security mission and success factors;
- Identify constituent elements of a security strategy and policy;
- Present a global approach for controlling information technology risks & security governance;
- Define security measures with a special focus on protection against system intrusion, crisis management, and disaster recovery plans;
- Propose an organizational structure for security management;
- Indicate the principal criteria for auditing and evaluating security levels.

At the end of the Cybersecurity Guide the reader will find a **glossary** of cybercrime and cybersecurity terms and an array of **relevant references**.

Table of Contents

PART I **1**

I. CYBERSECURITY CONTEXT, STAKES & CHALLENGES **2**

I.1 TOWARD AN INFORMATION SOCIETY 2
I.1.1 Information revolution *2*
I.1.2 Security in mind *3*
I.1.3 Innovation and development *4*
I.2 AVOIDING CYBERSECURTIY DIVIDE 4
I.2.1 Cybersecurity is essential for developing countries *4*
I.2.2 Cybersecurity for all! : so many challenges ! *5*
I.3 CYBERSECURITY FOR AN INCLUSIVE INFORMATION SOCIETY 7
I.3.1 Need for a global cybersecurity framework *7*
I.3.2 Need to enforce capacity building *9*
I.3.3 Need to raise awareness and developp a significant cybersecurity culture *10*
I.4 CYBERSECURITY STAKES 12
I.4.1 Cybersecurity objectives *12*
I.4.2 Cyber-insecurity exists! *13*
I.5 MULTI STAKEHOLDERS' INVOLVMENT AND PERSPECTIVES 14
I.5.1 Political dimension *15*
I.5.2 Business and economic dimensions *16*
I.5.3 Legal dimension *18*
I.5.4 Technological dimension *19*
I.5.5 Social dimension *21*

PART II **23**

II. CYBER TREATS, CYBER ATTACKS AND CYBER CRIME ISSUES **24**

II.1 UNDERSTANDING INTERNET TECHNOLOGIES 24
II.1.1 Telecommunication infrastructure and e-services *24*
II.2 FUNDAMENTAL PRINCIPLES IN TELECOMMUNICATION AND NETWORKING 25
II.2.1 Several types of networks *25*
II.2.2 Network components *25*
II.3 INTERNET: A NETWORK OF NETWORKS 26
II.3.1 Network access *26*
II.3.2 IP address and domain name *28*
II.3.3 IP & TCP/IP protocols *31*
II.3.4 Vulnerabilities of the Internet *32*
II.4 CYBERATTACKS 33
II.4.1 Passive and active attacks *33*
II.4.2 Denial-of-Service attacks *34*
II.4.3 Defacement attacks *36*
II.4.4 Malware attacks *36*
II.4.5 Cyber intrusion *42*
II.4.6 Spam and phishing *44*
II.4.7 Some communication protocols misuse *47*
II.4.8 Cyberattack methodology *48*
II.5 COMPUTER-RELATED CRIME AND CYBERCRIME 51
II.5.1 Definitions *51*
II.6 THE PRINCIPAL FORMS OF INTERNET RELATED CRIME 53
II.6.1 Swindles, Espionage and Intelligence Activities, Rackets and Blackmail *53*
II.6.2 Information Manipulation *53*
II.6.3 Economic Crime and Money Laundering *54*
II.6.4 Threats against States and cyber terrorism *54*
II.6.5 Crimes against persons *56*
II.6.6 Security incidents and cybercrime have to be reported *56*

PART III **59**

III. LEGAL, JUSTICE AND POLICE APPROACHES 60

III.1 COMPUTER FORENSIC 60
III.1.1 Computer investigation and digital evidence 60
III.1.2 Searching and collecting evidence 62
III.1.3 Collecting evidence in cybercrime investigation 64
III.1.4 Computer crime investigation methodology 66
III.1.5 ICT security manager and ICT police investigator collaboration 68
III.2 THE LEGAL DIMENSION OF CYBERSECURITY 69
III.2.1 Needs for a legal framework 69
III.2.2 Convention on cybercrime 69
III.2.3 Some law domains related to cybersecurity issues 72
III.3 SOME E-COMMERCE RELATED LEGAL ISSUES 73
III.3.1 Cyberspace and intellectual property: some basic considerations 75
III.3.2 Some legal considerations related to spam 77
III.3.3 Summary of the main legal issues relating to cyberspace 79
III.4 PRIVACY ISSUES IN THE INFORMATION SOCIETY 80
III.4.1 Privacy definition and main issues 80
III.4.2 Privacy stakes and challenges 81
III.4.3 Needs, constraints, policies and tools 82
III.4.4 A way to preserve privacy 83

PART IV 85

IV. TECHNICAL APPROACH 86

IV.1 PRINCIPLES OF INFORMATION TECHNOLOGY SECURITY 86
IV.1.1 ICT security criteria 86
IV.1.2 ITC Security Domains 86
IV.1.3 Security Tools 89
IV.2 ENSURING CONFIDENTIALITY 90
IV.2.1 Symmetric or private key encryption system 91
IV.2.2 Asymmetric or public key encryption 92
IV.2.3 The best of symmetric and asymmetric systems 93
IV.2.4 Key management 94
IV.2.5 Public-key infrastructure (PKI) 94
IV.2.6 Ensuring proof of origin by digital signature 95
IV.2.7 Ensuring resources integrity 96
IV.2.8 Ensuring resource availability 99
IV.2.9 Ensuring a non-repudiation service 99
IV.3 IMPLEMENTING SECURITY WHILE ACCESSING RESOURCES 100
IV.3.1 Conventional access control 100
IV.3.2 Access control based on biometry 101
IV.3.3 Access control based on digital certificate 103
IV.4 IMPLEMENTING SECURITY DURING DATA TRANSFER 104
IV.4.1 Routing procedures and security 104
IV.4.2 Name server and security 105
IV.4.3 Secure IP Protocol (IPv6 & IPSec) 105
IV.4.4 Virtual Private Networks 106
IV.4.5 Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure HTTP (S-HTTP) 107
IV.4.6 Intrusion Detection 108
IV.4.7 Data filtering and environments partitioning 108
IV.5 RISKS AND BASIC SECURITY MEASURES RELATED TO E-MAIL AND E-COMMERCE 109
IV.5.1 E-mail security issues and solutions 109
IV.5.2 E-commerce security issues 111
IV.6 PROTECTION OF COMMUNICATION INFRASTRUCTURES 113
IV.6.1 Some protocols communication security issues 113
IV.6.2 Several levels of protection 114
IV.6.3 Systems and network management tools for security enhancement 115
IV.7 TOOLS ARE NOT ENOUGH 117

PART V 118

V. MANAGERIAL APPROACH 119

V.1 SECURITY MANAGEMENT OBJECTIVES AND DEFINITION 119
V.1.1 Security is a business enabler 119
V.1.2 Security is a endless and dynamic process 120
V.1.3 Security is a question of principles 121
V.1.4 Security is a question of perspectives 122
V.1.5 Security is a question of governance 123
V.1.6 Security is a question of measures 124
V.2 IDENTIFY AND MANAGE ICT RISKS 126
V.2.1 What is a risk? 126
V.2.2 From risk analysis to security policy and measures 127
V.2.3 Define a security policy and implement appropriate solutions and procedures 128
V.3 A STANDARDIZED APPROACH TOWARD SECURITY MANAGEMENT 129
V.3.1 Use international standards 129
V.3.2 Use common sense 132
V.3.3 Minimize the cost of security 133
V.3.4 From data sensitivity to data protection 135
V.4 SECURITY ORGANIZATIONAL STRUCTURE 136
V.4.1 Security organization 136
V.4.2 Security audit 137
V.4.3 Protection against intrusion and reaction to malicious incidents 139
V.4.4 Defining a Disaster Recovery Program 140
V.5 SOME BASIC RECOMMENDATIONS TO IMPROVE CYBERSECURITY EFFECTIVENESS 142

ANNEXES 144

Table of Figures

Figure I.1: Digital information 2
Figure I.2: Cybersecurity for an inclusive society 6
Figure I.3:Building blocks of cybersecurity culture 11
Figure I.4:The Internet infrastructure and the many origins of problems 13
Figure I.5: Several dimensions of a cybersecurity approach 15
Figure I.6: OECD principles for information security (July 2002) 19
Figure I.7: Basic ICT security criteria 20
Figure II.1: Accessing the Internet 27
Figure II.2: Internet – intranet – extranet 28
Figure II.3: DNS server tree structure 30
Figure II.4: Internet communication protocols 32
Figure II.5: Sources of vulnerability for the Internet 33
Figure II.6: Passive and active attacks 34
Figure II.7: Denial-of-service attack 34
Figure II.8: Spyware attack 41
Figure II.9: Phishing attack 45
Figure II.10: Cyberattack methodology 49
Figure II.11: Targets of cyberattacks 50
Figure II.12: The nature of computer – related crime 52
Figure III.1: Overview of a crime resolution process 61
Figure III.2: Computer crime investigation methodology 67
Figure III.3: Some computer and data related offences 72
Figure IV.1: Security criteria and system capacity 86
Figure IV.2: Computer Security Domains 87
Figure IV.3: Logical Security 88
Figure IV.4: Symmetric encryption 92
Figure IV.5: Assymetric encryption 93
Figure IV.6: Public key infrastructure 95
Figure IV.7: Digital signature 96
Figure IV.8: Digital fingerprint 97
Figure IV.9: Fighting against viruses 98
Figure IV.10: Basic components of logical control 100
Figure IV.11: Biometric access control 102
Figure IV.12: Establishment of a VPN using an IPSec communication channel 107
Figure IV.13: Functional structure of a firewall 109
Figure IV.14: Protocols secuirty levels 113
Figure IV.15: Different aspects of security architecture 117
Figure V.1: Main cybersecurity objectives 119
Figure V.2:Complementarily of security and quality approaches 119
Figure V.3: Security: an endless process requiring several capabilities 120
Figure V.4: Security: a necessary compromise 121
Figure V.5: Strategic, tactical and operational security aspects 122
Figure V.6: Risk and security in a dynamic context 123
Figure V.7: Security measures 125
Figure V.8: From risk analysis to adapted security services 127
Figure V.9: Risks and the security process 128
Figure V.10: Information Security Management System 130

Figure V.11: ICT security: a matter of common sense 132
Figure V.12: Classification: a tool facilitating the identification of resources'' protection level 136
Figure V.13: Reaction to an attack..... 139
Figure V.14: Structure of a business continuity plan and disaster recovery plan 141
Figure V.15: Design methodology of a disaster recovery plan (strategic analysis step) 142

PART I

CYBERSECURITY CONTEXT, STAKES & CHALLENGES

Part I identifies the context, stakes and challenges of cybersecurity. The purposes of this part are to:

- Indicate some information society considerations and changes implied by the use of information and communication infrastructures;
- Identify the stakes, challenges and issues related to cybersecurity for developing countries;
- Define the main characteristics of cybersecurity; and
- Present the fundamentals of a global cybersecurity approach and the ITU Global Cybersecurity Agenda initiative.

I.1 TOWARD AN INFORMATION SOCIETY

I.1.1 Information revolution

Information and communication technologies (ICTs) are transforming the way we think about and do almost everything in our lives. They are bringing about important structural changes, by allowing us to model *objects* of all kinds in the form of information, and hence, manipulate them electronically. *Digitization* creates a digital image of something real, i.e. a "*virtual version*" of the object. All information – whether it takes the form of voice, data, or image – can be digitized and represented in some standardized manner.

The real technology revolution was brought about by the *digitization of information*, and its consequences go far beyond the world of telecommunication. Digitized information becomes disembodied, that is, it is no longer tied to the medium in which it is represented and stored. The value is the information itself (*content*) and do not provide from its physical medium (Figure I.1).

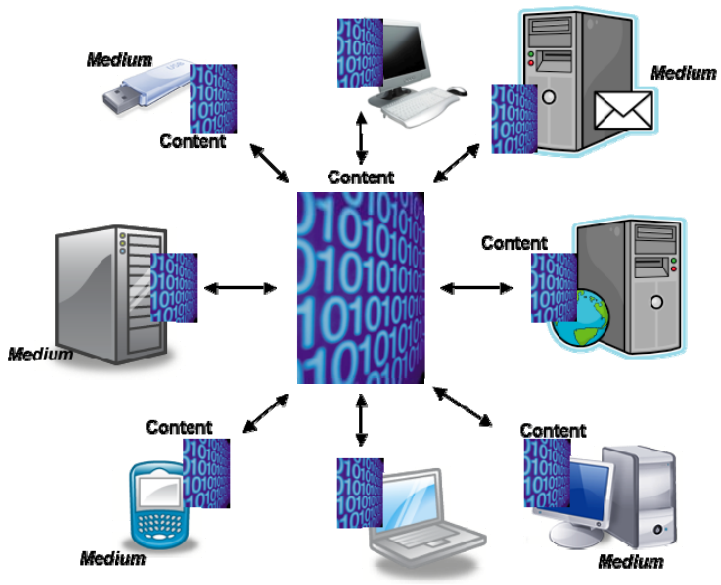

Figure I.1: Digital information

Data can be localized and processed in several places at once. The possibility of perfect duplication *ad infinitum* imperils the notion of "original" data, with potentially troubling implications for the concept of copyright protection.

Digital technology has made it possible to construct a continuous digital information chain, because it has standardized data production, processing and transfer (*digital convergence)*. Controlling the *digital information chain*, i.e., the infrastructure and the content, has become the major challenge of the 21st century. The new market, open to all, is characterized by the unprecedented mobilization of all players on a global level: telecommunication operators, cable operators, hardware and software manufacturers, service providers, television broadcasters, multimedia industry, etc. Unrestrained competition and the reorganization of roles and activities have created the new economic challenges for today's organizations.

When Gutenberg created the printing press, he had no way of imagining the repercussions that his invention would have on the future of industry. There was no way that he could have foreseen that his invention was the first step on the road to industrial automation. Something similar happened at the end of the 1960s. Universities and military users, each motivated by their own objectives, have set up a communication network that would eventually become the Internet. Like their predecessors of the 15th Century, they had no way of predicting the broader consequences of their creation. Today, ICTs and the cyberspace herald the transition of societies to the information age.

The *information revolution* profoundly alters the way information is processed and stored. It changes the way organizations, and indeed society as a whole, function. It is not the only technical innovation of this era, but it stands out because of its impact on the processing of *information*, and hence, of *knowledge*. The information revolution can be viewed as the wellspring of future *innovation*, because it affects the mechanisms by which knowledge is created and shared.

The use of information and communication technologies (ICTs) leads to a genuine evolution of the way politic, economic, social and cultural exchanges can be done, through a telecommunication network, in which the security of the flow of information needs to be ensured. No form of economic activity can exist without exchanges and interaction between the participants; no exchange of information is possible without some basic security guarantees; and no service can be planned without taking into account the need for quality of service. However, the success of a communication depends on the ability of the parties involved to deal with the technical constraints and manage the customs that any exchange of information involves.

I.1.2 Security in mind

The transformation of societies into an *information society*, made possible by the integration of information and communication technologies in every sphere of activity and every type of infrastructure, *increases the dependence* of individuals, organizations and countries on information infrastructures. This is a major source of *risks*, which must also be treated as well as those linked to cyberthreats, as a security risk. With the growing utilization of ICT, the existence of a global and interdependent information technology infrastructure, and the emergence of new threats, mastering operational computer risks is nowadays fundamental.

There is a danger that developing countries will put too few of their resources into security infrastructure as they attempt to join the information society. As a consequence, the *digital divide* could give rise to a *security divide*. There is also the danger that developing countries may become overly dependent on the entities that provide their means of cybersecurity[1].

The dictionary tells us that “security” is the protection against something bad that might happen in the future. Based on this basic definition, the concept of cybersecurity applied to the protection of any material or immaterial ICT resources against potential danger. A *danger* or a *threat* is the possibility of something happening (attack, error, dysfunction, natural catastrophe, …) that will injure, damage or destroy an ICT resource. *The threat could have a criminal origin or not, could be intentional or not.*

The telecommunication infrastructures and the services and activities that they make possible have to be conceived, designed, set up and managed with *security in mind*. Security is the cornerstone of any telecommunication activity; it should be viewed as a service that makes it possible to create other services and generate value (e.g. e−government, e−health, e−learning, …). It is not a matter of technology alone[2]. Until now, however, the basic communication tools that have become available have not included the resources that are both necessary and sufficient to provide or to guarantee a minimum level of security.

---

[1] S. Ghernaouti-Hélie: "From digital divide to digital unsecurity: challenges to develop and deploy an unified e-security framework in a multidimensional context", in *International Cooperation and the Information Society*, section of the Swiss development policy directory, IUED publications. Geneva, November 2003.

[2] A. Ntoko: "Mandate and activities in cybersecurity – ITU-D". WSIS thematic meeting on cybersecurity. ITU, Geneva 28 June-1 July 2005.

I.1.3 Innovation and development

Organizations and countries need to focus on the capacity to innovate and adapt rapidly. They must be backed up by a powerful and secure information and communication infrastructures, if they wish to survive and assert themselves as long-term players in the new *competitive environment*.

New areas of activity are being opened up by the diversification of telecommunication and the possibilities created by extended information technology, the benefits of which should accrue to the developing countries, too.

The technological and economic improvements made possible by the deployment of reliable ICT infrastructures holds great promise for ordinary people. At the same time, however, they introduce an unprecedented degree of technological and management *complexity*. The associated significant risks must be kept under control, to avoid vitiating the very notion of progress. With *technological risk*, e.g. a failure of information processing and communication systems, brought about by a malfunction of accidental or malicious origin, comes an *informational risk*, liable to undermine an organization's ability to make use of information.

While access to ICTs is widespread and growing, a far from negligible part of the population remains excluded from the information revolution. The reasons for this include *cultural and financial factors*, and, in some cases, basic difficulties such as lake of resources, competencies or illiteracy. More than in any other domain, *training and education are crucial* to democratizing ICT and combating *info-exclusion*. The communication interfaces will also need to be thought anew so as to serve the population better and respect the diversity of cultural contexts.

ICTs, like all technologies, emerge and operate in a particular *historical* and *geographical context*. The responsibility of policymakers is to support the information revolution with the tools, procedures, laws and culture needed to deal with security and meet the *expectations and needs of a given society*.

Developments in ICT and the way people use them have outpaced the regulations that govern them. There is therefore a *need for an appropriate legal framework* to be put in place to address such issues as for example: the aterritorial nature of the Internet, the problems of responsibility, consumer and children protection or the protection of privacy and of property rights.

Technological evolution needs to be paralleled by an evolution of the social, political and legal order. This cursory consideration already gives an idea of the importance of the challenges created by the *information age*, the crucial role of telecommunication in meeting them, and the importance of dealing with security issues before they become a hindrance to development.

The transition to the information age reveals the importance of information technology and makes it clear that the technology needs to be mastered. Considering the new dimensions that ICT creates, in technical and socio-economic terms, *cybersecurity* has become a *fundamental need*. It highlights the strategic and critical nature of what is at stake in planning and implementing cybersecurity, for countries, for organizations, and for individuals.

I.2 AVOIDING CYBERSECURTIY DIVIDE

I.2.1 Cybersecurity is essential for developing countries

In today’s world, there is widespread system interconnection, increasing linkage between infrastructures, and growing dependence on digital technologies -- and the growth of threats and risks that go along with these things. This makes it necessary for individuals, organizations and countries to take steps to adopt measures, procedures and acquire tools to improve the way that technological and cyber-risks are managed. The struggle to contain technological risk is at the heart of the challenges facing us in the 21st century. It calls for a *comprehensive global approach* to security that will include the developing countries.

The ability to provide security for information, processes, systems and infrastructure is crucial to the success of a given economy. In particular, it is essential for the developing countries to build off of the experience acquired in the developed countries. It is essential to ensure that cybersecurity does not become another dividing line between the haves and the have-nots.

It is not enough to set up points of access to telecommunication networks. It is necessary to deploy ICT infrastructures and cyber services that are reliable, maintainable, robust and secure, while respecting basic human rights and the rights of states. The need to protect systems and valuable information has to coexist and be harmonized with the parallel protection of the rights and privacy of individuals.

Digital divide should not be double by a security divide. Security needs should be answered at the same time than ICT development. Any ICT infrastructure should integrate basic security services. At this condition developing countries could take advantage of the information society. Avoiding becoming a digital paradise or the weak link of the *international security chain*, contributes to be an important economic development actor.

I.2.2 Cybersecurity for all! : so many challenges !

Each actor dealing with information and communication device, tool or service, for professional and/or private issues is concerning by the cybersecurity issue. It concerns: governmental institutions, big or small organisations and individuals. It should be noted that a security approach is often limited to the installation of risk reduction measures to protect information technologies resources of large organizations. However, the security approach must also meet the security needs of small and medium organizations and of individuals.

Any comprehensive approach toward cybersecurity must grapple with such imposing issues as states' sovereignty, national security, the cultural heritage of nations, and the protection of critical infrastructure, systems, networks, goods and values – and the safety of individuals.

The security answer should satisfy particular *protection and defence* levels requirements, in regards of the actor's need. Because *humans are the weakest link of the security chain* and because human is the final "consumer" of ICT service, infrastructures and of cybersecurity, any security solution should also take into consideration social and societal needs. The individual should be at the heart of any ICT security question, to help realize a conscious and inclusive information society (Figure I.2).

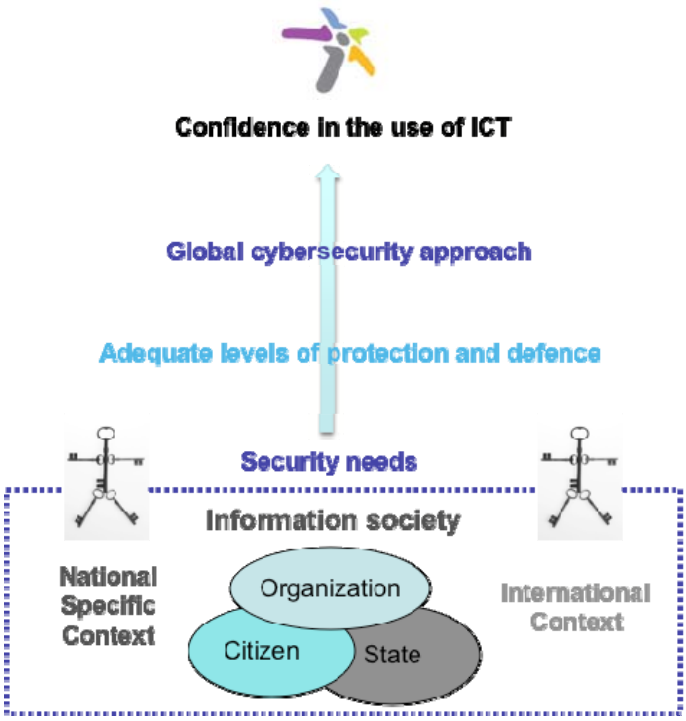

Figure I.2: Cybersecurity for an inclusive society

Cybersecurity includes topics related to cybercrime issues and to potential ICT or security misuse, but cybersecurity is not only fighting against cybercrime. Cybersecurity deals also with the fact that technologies should be less vulnerable.

Cybersecurity also concerns:

- Producing secure, transparent and third controlling products;
- The development of a reliable and safe behaviour in regard of the use of ICT;
- The development of a legal framework enforceable at national level and compatible at international level.

It is illusory to think that technological or legal solutions will compensate for design or management errors whether they occur at strategic, tactical, or operational levels.

The legal and technological worlds must be in harmony. Technology is not neutral, nor is the law.

Let us make it such that their development follows economic development, and that they become a driving force for the economy of nations.

For developing countries as for others, *carrying out activities over the Internet* presupposes that four major issues have been resolved, namely:

First, network infrastructure should exist with if possible; high-speed data transfer capabilities and quality of services. The cost of use should be affordable and in correlation with the performances and quality of service obtained. That implies having a valid underpinning economic model and an effective cost management process.

Second, contents and services should meet users' needs in term of pertinence, quality, flexibility and accessibility. As previously stated, cost must be effective.

Third, e-services should be reliable and trustworthy, integrity, confidentiality, authenticity and availability security criteria have to be guaranteed. Furthermore, traceability and proof must be possible for third party control.

Security and trust are relative notions but they are critical factors of success and business enablers for developing the information society. The underlying problem is to be found at the level of security and confidence offered and guaranteed through access, services as well as by information and communication technologies providers. That could be summed up by the question "*Who controls infrastructures, access, use, services, content and security?*"

Just as we trust in air transportation we must have confidence into information and communication technologies. This is only possible by implementing tight and rigorous control processes and by ensuring that security measures are implemented in total transparency.

Fourth, an enforceable legal framework should exist and laws should be updated to adequately cover extensive use of data processing and telecommunications. Procedural standards should be defined to allow governments' access to stored or transmitted data, while taking privacy protection, civil liberties and public safety into balance. In addition, justice system representatives, the police force, investigators and lawyers must be trained to deal with acquisition, preservation, analysis and interpretation of digital evidence. Nowadays there seems to still be a general lack of coordination and harmonization of legal frameworks.

The real challenge for developing countries is to keep *security* handling *simple* and *cost-effective*. Security mechanisms and tools should be:

- Readily understood;
- Configured with a minimum of effort by untrained users;
- Transparent for the end-user (Third party control possible);
- Flexible and manageable for information technologies' providers;
- Designed with the right balance between efficiency, configurability, usability and costs;

Managing information risks through cybersecurity could help to strengthen *confidence* in the electronic marketplace of emerging countries, but at the same time cyber security should not become an obstacle to the entrance of emerging economies onto the cybermarket.

There is no real technical obstacle to further development of cybersecurity but the scope of deployment of effective local and international security services is very *complex* and technical and management costs are not minor. Private and public partnership is desirable, at national and international levels, to integrate security into infrastructure and to promote a security culture, behaviour and tools. Business, financial and organizational models are to be found to support effective deployment of security that could be of benefit to everyone.

I.3 CYBERSECURITY FOR AN INCLUSIVE INFORMATION SOCIETY

I.3.1 Need for a global cybersecurity framework

ITU (*International Telecommunication Union*) was entrusted to take the lead as sole facilitator for Action Line C5, "Building confidence and security in the use of information and communication technologies (ICTs)" at the second phase of the WSIS in Tunis in 2005.

ITU Membership has been calling for a greater role to be played by ITU in matters relating to Cybersecurity through various Resolutions, Decisions, Programs and Recommendations Together with partners from governments, industry, academic and research institutions, regional and international organizations as well as individual experts all over the world.

For that, ITU has established a global framework for international cooperation in cybersecurity: The **Global Cybersecurity Agenda** - – ITU GCA[3]

The five domains of Global Cybersecurity Agenda are: *Legal Measures*; *Technical and Procedural Measures*; *Organizational Structures*; *Capacity Building* and *International Cooperation*. Theses domains constitute the five chapters of the global strategic report– A framework for international cooperation in cybersecurity[4] available since November 2008.

Work as started October 2007 by setting achievable goals in order to contribute to elaborate global strategies for:

- The development of a model cybercrime legislation;
- The creation of appropriate national and regional organizational structures and policies on cybercrime;
- The establishment of security criteria and accreditation schemes for software applications and systems;
- The creation of a global framework for watch, warning and incident response;
- The creation and endorsement of a generic and universal digital identity system;
- The facilitation of human and institutional capacity-building;
- The international cooperation, dialogue and coordination.

The *global information society* and *knowledge economy* are constrained by the development and overall acceptance of an international cybersecurity framework. The validity of such a framework or model requires a challenging *multidimensional cybersecurity approach* for everyone – from individuals to organizations and states.

It is fundamental that the international community, including developing countries:

- **Understand** cybercrime from a global perspective;
- **Define a national cybersecurity strategy**;
- **Develop public awareness** of cybercrime and cyber security challenges (economic and management issues, political issues, social issues, technical issues, legal and law enforcement issues);
- **Promote a cyber security culture** (information on stakes and risks, dissemination of simple recommendations, such as: use secure systems, reduce vulnerability by avoiding dangerous situations or behaviour, etc.);
- **Train and inform** on information and communication technologies and on security issues, and relevant legal provisions;
- **Develop cyber security education**;
- Propose a **unified cybersecurity framework** which includes, in a complementary fashion, the human, regulatory, organizational, economic, technical and operational dimensions of cyber security;
- Put in place **organizational structures** to support a national cybersecurity strategy;
- **Create regional alert points** for the provision of technical information and assistance regarding security risks and cybercrime;

[3] www.itu.int/osg/csd/cybersecurity/gca/

[4] See the report: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

- Create **effective** cybercrime **laws** that are enforceable at national and international levels (global and harmonized legal framework taking into account the right to privacy (Protection of public safety, with protection of privacy and civil liberties));
- Redefine **law enforcement and legal framework** in order to bring cybercrime perpetrators to justice;
- **Manage jurisdictional issues**;
- **Fight cybercrime** (deterrence, detection, investigation, prosecution of cybercriminal activities, crime reporting, crime analysis, practices and experiences on search and seizure of digital evidence, organizing capacities to combat cybercrime, information sharing, promotion of effective public and private sector cooperation);
- **Develop acceptable practices** for ICT protection and reaction;
- Establish **effective cooperation** and promote cooperation and coordination at national and international levels;
- Force information technology and content providers to **improve** the **security** of their products and services. Products or services must integrate, in native, simple and flexible security measures and mechanisms. Products should be well-documented and comprehensible and security mechanisms should be readily understood and configured easily by untrained users. Security must be integrated at the beginning of information technologies' infrastructure development life cycles.

I.3.2 Need to enforce capacity building

Capacity building contributes to the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation, human resources development and strengthening of managerial systems.

Capacity building includes:

- *Human resource development*, the process of equipping individuals with the understanding, skills and access to information, knowledge and training that enables them to perform effectively;
- *Organizational development*, the elaboration of management structures, processes and procedures, not only within organizations but also within the management of relationships between the different stakeholders (public, private and community);
- *Institutional and legal framework development*, making legal and regulatory changes to enable organizations, institutions and agencies at all levels and in all sectors to enhance their capacities.

Within the context of the **Global Cybersecurity Agenda**[5], the main goal related to capacity building is: "Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas."

The main components of the capacity building in cyber security are various awareness raising initiatives, resource building and training.

Capacity building measures goes far beyond awareness and requires specific resources (financial, technical, human resources), *know how sharing* and *international cooperation*. *Economical models* have to be developed to support cybersecurity capacity building actions as well as to support improvement of existing capacities. *Developing and least-developed countries could need helps to build cybersecurtiy capacities.*

[5] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

Educational efforts and investments need to be made to educate and train all the members of the information society: from decision makers to citizens. Specific actions should be taken at a national level, to raise or build cybersecurity capacities of various actors in order to be able to deal with national and international cybersecurity issues. *Awareness-raising*, as well as specific education programs, is difficult to achieve and is costly. As capacity building activities take place at national level, appropriate resources should be found consequently. For that, financial, technical, organizational and human resources should exist. In some specific contexts, developed countries should benefit from international cooperation. At the same time, **awareness is not enough** to *empower the end-user* in a way that he or she would be able to adopt a safe and responsible behaviour when dealing with ICT technologies. Specific educational programmes should be effective and available for each kind of stakeholder (policy makers, justice and police professionals, managers, information technology professionals and end-users. At the very beginning of these programmes, cybersecurity training courses should be integrated into different levels of educational courses, from school to university, and including education in the legal, scientific and social science fields.

Developing interdisciplinary training of cybersecurity will be a real added value activity, permitting people to deal with a large range of cybersecurity issues. *Continuous training* should not be omitted, in order to prepare professionals to face the evolving and dynamic context of technology and threats.

Effective Capacity building measures should also contribute to help to create a more difficult digital environment to attack by decreasing the number of vulnerabilities of potential targets.

Capacity building measures are pro-active actions and rely upon:

- A good understanding of the role of cybersecurity's actors (including their motivation, their correlation, their tools, mode of action) and of ICT related risks;
- Complementary technical, legal, organizational measures;
- Efficient ICT security and quality management approaches;
- Efficient national, regional, international cooperation.

I.3.3 Need to raise awareness and developp a significant cybersecurity culture

Protecting the information is a crucial issue to take into consideration in developing the information society. At the crossroads of technological, legal, sociological, economic, and political fields, cybersecurity is an interdisciplinary domain by nature. Depending on the country, a national cybersecurity approach must reflect the vision, the culture and the *civilization of a nation* as well as meeting the *specific security needs of the local context* in which it is introduced.

Because cybersecurity has a *global dimension* and deals with a large range of issues as:

- ICT uses or misuses;
- Technical measures;
- Economic, legal and political issues;

it is important to develop a general *cybersecurity culture* in order to raise the level of understanding of each member of the cybersecurity chain.

A cybersecurity culture deals with key economic, legal, and social issues related to information security in order to contribute to helping countries get prepared to face issues and challenges linked to information and communication technologies (ICT) deployment, uses and misuses."[6]

Figure I.3 points out the main building blocks needed to successfully promote a culture of cybersecurity.

[6] S. Ghernaouti-Hélie - "Information Security for Economic and Social Development" UNESCAP – 2008 http://www.unescap.org/icstd/policy/

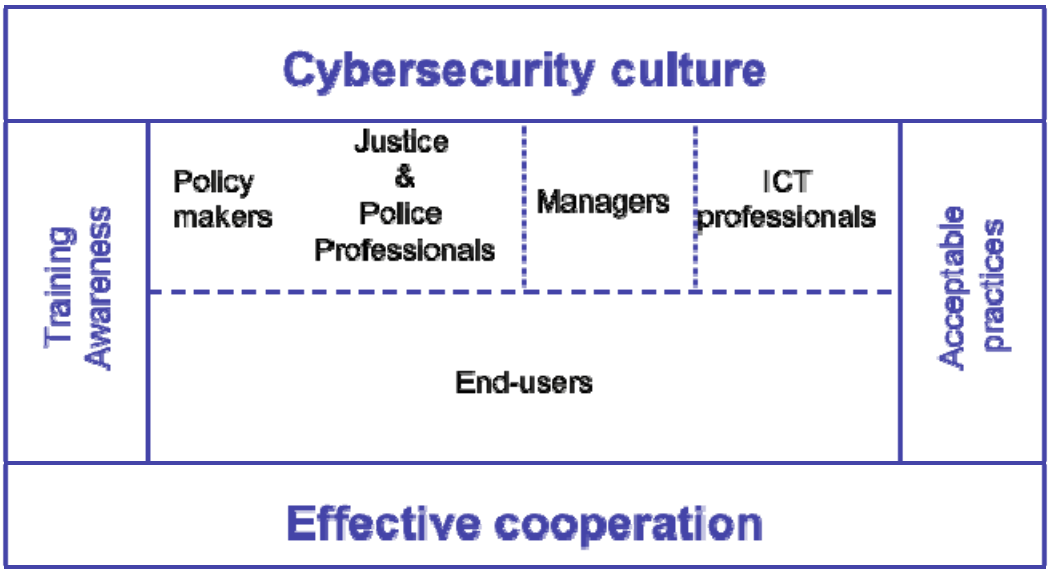

Figure I.3:Building blocks of cybersecurity culture

Answering a global challenge by a local answer: the ICT level of penetration or Internet uses can vary from country to country, and even if cybersecurity problems are similar, the way to deal with those problems will depend, for example, on local culture, contexts, and national legal frameworks. But even if each country is different, some countries at a regional level might have the same level of Internet penetration and have similar cybersecurity needs. So sometimes, having a regional answer could be appropriate in specific contexts. Any global strategy to develop a cybersecurity culture has to be adapted to local needs.

When developing cybersecurity culture, one of the main challenges is to identify correctly what are the global and international issues and what are the local specific needs for a cybersecurity culture.

International standards can only contribute to identifying the global and generic main issues related to a cybersecurity culture because cultures rely upon local and temporal factors. A unique and exclusive cybersecurity culture could be prejudicial to specific information society environments and visions. It could fail to respond adequately to the multitude of end-user backgrounds, points of views, and needs.

Promoting a culture of cybersecurity that will touch the entire population needs to rely upon an appropriate *political vision and will* and *efficient private and public partnerships*. It is too soon yet, to assess the long term effects of the several existing awareness and educational initiatives. There are no real theories or methodologies related to how to design, to communicate, to validate or to control the adequacy of a cybersecurity culture. Evaluating the effectiveness of cybersecurity culture, from policies and guidelines to practice, is very difficult. But at the same time we know that if the public and private sectors do not support such initiatives together as soon as possible, there will be a long term negative effect on economic development and the ability to ensure the security of goods and people.

Let us remember the following guidelines from the Organization for Economic Co-operation and Development; *OECD's 2002 guidelines for the security of information systems and networks* – "Towards a culture of security"[7], which are a starting point for examining security issues. The first two points mentioned are:

[7] www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf

- "**Awareness**: Participants should be aware of the need for securing information systems and networks and what can be done to enhance security;
- **Responsibility**: All participants are responsible for the security of information systems and networks".

There is a global *responsibility* to provide citizens with the appropriate information related to cybersecurity issues. Sufficient awareness and education will contribute to that and to prevent incompetent or incorrect behaviours. It will also assist the development of trust and confidence in ICT infrastructures, services, security mechanisms and controls. It will also avoid building security based on fear. Fear is a selling argument when dealing with security issues but is not always rational and does not lead to the best investments and efficiency in security. It can, however, be synonymous with excessive control that will impact the preservation of human rights and privacy.

People should be able to develop their own approach to, and informed assessment of, how they should behave in respect of cybersecurity and the use of ICT. It is everyone's responsibility to promote *a safe and reliable cyberspace* environment in the context of an emerging information society.

Every citizen should:

- Understand the cyberthreats for the end-user (viruses, spam, identity theft, fraud, swindle, privacy offence, etc…) and their impacts;
- Understand how to adopt a security behaviour for a safe use of ICT resources;
- Be able to promote a cybersecurity culture based on well-recognized good practices.

There is a global responsibility to contribute: (i) to help developing countries find their own good practices by transferring knowledge and skills; and (ii) to equip developing countries with the means for developing an economy of service. For developing countries, the information society could be an unprecedented opportunity to provide an alternative to the exploitation of their natural resources.

So to empower human resource in a global perspective, a general, modular and flexible educational framework in cybersecurity should exist to answer the needs of increased public awareness and provide a deeper education for particular professionals. This concerns both well-developed countries and less developed ones.

Because *education* is a key factor to strengthen competitiveness, employment and social cohesion, education is the key factor in becoming an actor in the information society and it constitutes the cornerstone of a knowledge-based society. Therefore, to enhance confidence and security in the use of ICT and cybersecurity, education should not be considered merely as an option. Education contributes to developing a layer of defence in deep security approach and is the cornerstone of the information society. Education constitutes a real human capacity challenge that governments have to face.

Promoting a culture of cybersecurity contributes to building a safe and inclusive information society. Considering cybersecurity education is a long-term approach which is efficient for a sustainable information society.

I.4 CYBERSECURITY STAKES

I.4.1 Cybersecurity objectives

Mastery of digital information wealth, distributing intangible goods, adding value to content, and bridging the digital divide are all problems of an economic and social nature, which call for something more than a one-dimensional, strictly technological approach to cybersecurity.

The ultimate objective of cybersecurity is to ensure that no lasting harm is done to the individual, the organization or to the state. This consists of the following: (i) protecting values (ii) reducing the likelihood that a threat materializes; (iii) limiting the damage or malfunction resulting from an

incident; and (iv) ensuring that, following an incident, normal operations can be restored within an acceptable time-frame and at an acceptable cost.

The cybersecurity process involves the whole of society - every individual is concerned by its implementation. It can be strengthened by developing a *cyber code of conduct* and a genuine national cybersecurity policy.

I.4.2 Cyber-insecurity exists!

The security deficit in ICTs is a reflection of the nature of information technologies and of cyberspace. The fact that users move in a virtual world, acting remotely and relatively anonymously, compounds the difficulties of designing, implementing, managing and controlling this technology. When one adds *failures, malfunctions, errors, mistakes, inconsistencies* and even *natural disasters* into the equation, the result, not surprisingly, is an aura of *insecurity* that haunts the ICT infrastructure (see Figure I.4).

Figure I.4:The Internet infrastructure and the many origins of problems

In this environment, there are many ways in which a malicious attacker may exploit vulnerabilities[8]. The list of these types of attacks is long. It includes identity theft, system spoofing, intrusion, resource hijacking, infection, deterioration, destruction, tampering, breach of confidentiality, denial of service, theft, and extortion. The proliferation of such attacks illustrates the limitations of current security strategies, but also, paradoxically, shows that the infrastructures have certain robustness.

Whatever the motivations of individual computer criminals may be, the results always include a far from trivial economic impact. Cybercrime is fast turning into an international hydra-headed monster.

Security strategy is often limited to a purely technological approach of setting up mechanisms to reduce the risks to which the organization's information assets are exposed. A more effective approach

[8] Cybercrime, cyberattacks and cyberoffences are discussed in depth in Part II.

is to take into account all the dimensions of the problem and address the security needs of individuals, especially the protection of privacy and basic rights. Cybersecurity should cover everyone, and it should extend protection to data of a personal nature.

Security solutions do exist, but they are never definitive, and generally represent no more than a response to a particular problem in a specific context. In many cases they are purely technological in nature, addressing a particular problem in a specific context - and, like all technology, they are fallible and can be circumvented. Usually they merely *displace the security problem* and *shift responsibility* to another part of the system they are supposed to protect. Furthermore, they are themselves in need of protection and secure management. At best, they represent a tentative attempt to deal with a dynamic reality of fluid technology, shifting targets, evolving hacker skills, and mutating threats and risks. There is *no guarantee* that a particular approach to security will provide lasting protection, or a return on the investment it requires. Another problem is that the proliferation of heterogeneous solutions may harm the overall coherence of the security strategy. Clearly, *technology alone will not suffice*; it must be integrated within a broader managerial approach.

Overall security strategy coherence is complicated by the wide range of different entities and individuals involved. This includes engineers, developers, auditors, systems engineers, legal experts, investigators, clients, suppliers, and users. It is complicated too by the broad array of interests, visions, environments, and languages. The digital economy will only be secure if there is a unified, systemic grasp of security risks and measures, and a recognition of the respective responsibilities of all parties involved.

I.5 MULTI STAKEHOLDERS' INVOLVMENT AND PERSPECTIVES

Social issues, the economy, public policy, human issues: whichever way one looks at it, and whether one calls it computer or telecom security, cybersecurity touches on the security of the digital wealth of people, organizations and countries (Figure I.5). The challenges involved are *complex*, and meeting them requires the political will to devise and implement an overall strategy for the development of information infrastructures that includes a coherent and effective cybersecurity strategy. A strong response to the human, legal, economic and technological dimensions of information infrastructure security needs can build confidence and generate welcome economic growth benefiting all of society.

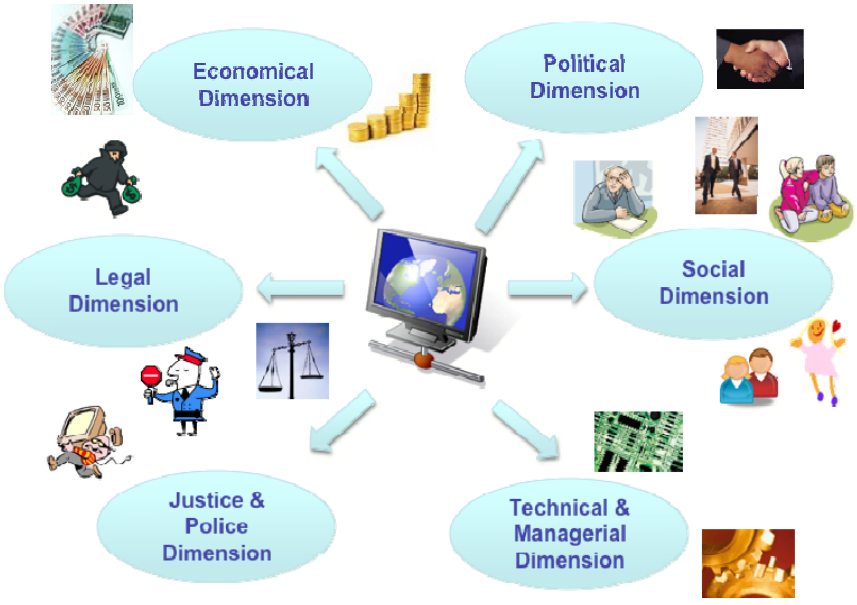

Figure I.5: Several dimensions of a cybersecurity approach

I.5.1 Political dimension

Because Cybersecurity and cybercrime issues are governmental issues, and national security issues, government people should understand:

- Links between social and economic development with crime and security issues in a connected society with interrelated infrastructures;
- ICT related threats and risks for states, organizations and citizens including privacy and economic crime issues;
- Needs for protection at national, regional and international levels;
- The role of all relevant stakeholders and relationships between private and public sectors;
- To define general measures to be taken to obtain a satisfying level of ICT security and protection assets (including privacy issues);
- How to create, maintain and develop trust in ICT environment;
- How to develop strategic improvement in ICT security.

These are some conditions among others, without forgot the necessary budget to be made available to sustain security measures and organizational structure.

The state possesses considerable responsibility for making digital security a reality. This is particularly true for the definition of an appropriate legal framework - one that is unified and practical. It should also promote a security culture and demand compliance with security standards, while strengthening law enforcement in respect to cybercrime. This raises the question of the underlying financial model and public-private partnership for national and international action plans.

At the strategic level, it is necessary to:

- Develop a national cybersecurity strategy;
- Implement a national strategy;
- Build national incident management capability;
- Ensure prevention, reporting, information sharing and alert management;
- Raise awareness of best practices in risk management and security;
- Develop an efficient legal system;
- Deter cybercrime;
- Provide assistance regarding the promotion of law enforcement and security;
- Encourage cooperation among several stakeholders and between private and public sectors.

However, security and deterrent measures are not enough. It is also essential for the state to provide education, information, and training in information processing and communication technologies. Building awareness of security issues should not be limited to the promotion of a particular security culture and cyber code of conduct. The security culture must be underpinned, upstream, by an IT culture.

The state must give the different players the means by which to learn to manage the technological, operational and information risks that threaten them in connection with the use of new technologies. In this context, the state must also encourage the reporting of instances of cybercrime. It must ensure that there is trust between the various players of the economic world and the legal and law-enforcement authorities.

Those authorities, along with the civil-defence authorities, emergency services, armed forces and security forces, have a tactical and operational role to play regarding the protection, prosecution and reparation of cybercrime. The state must ensure that organizational structures as surveillance, detection or information centres for ICT and criminal risks exit and are made operational.

It is up to each state: (i) to define a development policy for the information society reflecting its own particular values; and (ii) to provide the resources necessary to make it a reality, including the means for protection.

To contain cybercrime in a global, centralized and coordinated manner, states need to have a response at the political, economic, legal, and technological levels - a single response that can be adopted by all of the players in the digital chain as fellow partners in security.

The desire for simplicity and effectiveness in security is at odds with the complexity of needs and environments. This makes the outsourcing of services and system and information security to specialized providers more attractive. The tendency to outsource creates a high, or in some cases, total degree of *dependence*. This is a major *risk* for state sovereignty. States must beware of becoming dependent for the strategic, tactical and operational management of their cybersecurity on external entities that are beyond their control.

The *Internet* is on the way toward becoming a necessity of the information society. It could be viewed as a *critical infrastructure*, as essential as the electric distribution systems. The capacity of companies to produce and carry out services is increasingly related to technologies and services provided by the Internet. The concept of criticality associated with information or, more generally with an infrastructure, relies on its importance level and determines the survival of those whom depend on it. However, the data processing and telecom infrastructures belong only partially to those who depend on them. Even the so-called "public" infrastructures belong to a large extent to private companies, so public and private partnerships should be well defined.

In this context of *dependence and interdependence* of telecommunication and electric infrastructures, the protection of critical infrastructures including information infrastructures, is important for any national economy.

Availability, reliability, confidentiality, integrity, quality and confidence seem to be criteria that one wishes to be able to associate with any type of electronic services whether in the context of the *cyber-administration*, e-government or in that of the trade and finance. *Information security* is the essential basis of the success of Internet for the use of states, organizations, and citizens.

Policymakers also need to implement legal measures that are harmonized with the mechanisms of security models. Those legal measures are essential to prevent and deter criminal behaviour that: (i) uses pervasive networks as a target of crime (new technology – new crimes); or (ii) uses pervasive networks as a means to realize a crime (old crime with new technology). The legal dimension of cybersecurity should be viewed as a global business enabler that will contribute to minimizing criminal opportunities.

I.5.2 Business and economic dimensions

Considering cybersecurity from organizations points of view, executive managers of any size organization (including small and medium enterprises) should understand basic principles in ICT security management, in particular on the following topics:

- Assessments of vulnerabilities and threats;
- Security mission, management practices and conditions of success;
- How to identify valuable assets and related risks;
- How to define security policy;
- How to organize security mission, to control, to evaluate, to audit, to estimate cost;
- How to manage security in complex and dynamic environments.

In order to be able to:

- Produce effective security process and master ICT related risks and security costs;
- Collaborate with legal, law enforcement and technical professionals;
- Create appropriate organizational structures and procedures.

It may appear relatively straightforward to estimate what cybersecurity costs - associated budgets, cost of security products, training, etc. Assessing the profitability of security is more difficult. Taking a subjective approach, one might suppose that security measures intrinsically possess a passive form of effectiveness that prevents certain potential losses. Nonetheless, it is difficult to weigh the cost of security and the costs associated with losses due to accidents, errors or malicious acts. The cost of security depends on the assets that the organization needs to protect, and the cost of damage resulting from insufficient security. There is no ready answer to the following questions: What is the economic value of security? What is the return on investment of security?

The economic value of security must be conceived in the broadest social sense, taking into account the impact of new technologies on individuals, organizations and nations. It cannot be reduced to the costs of installation and maintenance of security tools.

A number of bodies of national law and international conventions legally bind organizations to put into place security measures. Those laws create obligations on the part of managers of organizations and their security administrators, to implement security measures (but not an obligation in terms of results). An entity that is guilty of a security lapse leading to an infraction may have a responsibility of a criminal, civil or administrative nature. Whether or not such responsibility is established will, of course, have no bearing on the criminal responsibility of the individuals who are guilty of the infraction.

The *need to integrate a legal dimension* relating to data processing is being increasingly felt by organizations. This relates to data conservation, responsibility of technical staff, management of personal data, cyber monitoring of employees, intellectual property, ICT contracts, E-commerce, etc. and regulatory compliance …

The *legal conformity aspect* of information systems is a new dimension that must be taken into account by persons in charge of data processing. Thorough knowledge of new technology-related laws becomes a necessity, and the law must be borne in mind when installing security solutions. Legislation indeed becomes an endogenous factor when considering security.

In the developed countries, omnipresent legislation in information systems governance can become a *strategic asset* for organizations that manage them, and legal intelligence constitutes a key factor of success for companies' strategies. Thus, persons in charge of security for organizations must be sensitized to the constraints of police investigation (minimal documentation relating to incident, conservation of traces, etc.). This measure makes sense only when incidents are reported to the police. A country must support reporting cybercrimes and build confidence among the various actors of the economic world, the justice system and the police.

Appropriate legislation on data processing makes it possible to strengthen the economic partners' confidence in the national infrastructure. These laws help to create a favourable context for data exchange based on compliance with the law. They encourage the general public to adopt information and communication-based services. Legislation and security may be viewed as two levers of the national economy. Cybersecurity conceived in terms of confidence and quality, lays the foundations for the development of a sound service economy.

States and organizations must take steps: (i) to foster a culture of prudence regarding ICT usage; and (ii) to develop a multidisciplinary approach toward cybersecurity. They need to control the risk that ICTs will be used to criminal ends.

I.5.3 Legal dimension

Just as there are tax shelters, so there are legal safe havens. The proliferation of computer-related crime is not necessarily a sign that there are not enough laws. Existing laws already cover many of the activities of ICT criminals. Policymakers need to create new legislation to complement existing laws, which, of course, also apply in cyberspace.

It is not enough to strengthen legislation, if the means to apply it are not there. A law is of little use if law enforcement is not up to the task of gathering and analyzing evidence, and identifying and prosecuting the perpetrators of criminal acts. If a malevolent is confident that he/her will escape punishment, this is a strong indication that the law is ineffective.

Taking into account the legal dimension and specific needs for justice and police professionals, Global understanding of legal issues related to ICT technologies and misuses should well understand by professionals in the field of justice and police. Depending on their activities they should know for example:

- Legal requirements at national and international levels;
- Computer investigation and forensic methodologies and tools;
- How to interpret and implement existing international regulation as Cybercrime convention of Council of Europe (doctrine) that could be considered as an international reference model to develop legal frameworks and international cooperation;
- Etc.

Competent professionals should be able to define a legal framework with appropriate cyber laws enforceable at national level and compatible at the international level. Measures to fight against cybercrime should be developed, keeping in mind the international cooperation need.

Delinquents adapt to any new environment and take advantage of it to carry out their traditional activities. There is legitimate cause for alarm that these individuals can be so perversely creative when it comes to inventing insidious new uses for these technologies.

It would be dangerous for the police forces to postpone achieving competencies and resources to investigate computer crime. It would have a severe, direct financial cost - in the form of investment in new infrastructures. Even worse would be the social cost due to the increase of organized crime and other destructive activities with destabilizing effects.

However, a colossal increase of “police presence” on the network is not necessarily the best solution. It is essential to preserve bedrock democratic principles throughout the cyber world.

Effectively combating cybercrime requires a legal framework that has been harmonized at the international level and that can be applied effectively. It also requires true international cooperation at the level of the police and justice authorities. It is important that this legal framework respect individuals' rights to *digital privacy*, while *strengthening efforts to combat cybercrime*.

The principal objective of the struggle against cybercrime must be the protection of individuals, organizations and countries, bearing in mind the fundamental principles of democracy.

The tools used to combat cybercrime are potentially inimical to human rights, and may undermine the privacy of personal information. Security requires surveillance, verification and profiling. Checks and balances are essential if: (i) abuses of power and of position are to be prevented; (ii) the temptation of totalitarian methods resisted; and (iii) respect of basic rights guaranteed. Those basic rights include the right to cyberprivacy and the protection of confidential personal information.

The political will to deal with cybercrime exists at the international level. The problem is not always the absence of laws or guidelines, such as those promulgated by the Organisation for Economic Co-operation and Development (OECD) with its "OECD Guidelines for the Security of Information

Systems and Networks – Towards a Culture of Security – 2002[9]" (Figure I.6). Rather, it is the difficulty and complexity of the task, and the resources necessary to effectively combat, not only cybercrime, but also organized crime and terrorism, that results in the Internet being exploited for malicious purposes.

Awareness	All participants are responsible for the security of information systems and networks
Responsibility	All involved have a share in the security of systems and information networks
Response	Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents
Ethics	Participants should respect the legitimate interests of others
Democracy	The security of information systems and networks should be compatible with the essential values of a democratic society
Risk assessment	Participants should conduct risk assessments
Security design and implementation	Participants should incorporate security as an essential element of information systems and networks
Security management	Participants should adopt a comprehensive approach to security management
Reassessment	Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures

Figure I.6: OECD principles for information security (July 2002)

It is important to ensure that all internet stakeholders are: (i) aware of the importance of the security issues involved; and (ii) aware of the basic measures that, if effectively implemented, can strengthen user confidence in data processing and communication technologies. The Internet should be an asset for everyone and not a haven for ubiquitous criminal activity.

I.5.4 Technological dimension

Concerning the technology dimension of cybersecurity ICT professionals should:

- Understand ICT technical vulnerabilities and misuse;
- Understand ICT related risks, cyberthreats and cyberattacks;
- Understand societal and organizational issues and values.

In order to be able to:

- Decrease the number of vulnerabilities of digital environments;
- Define, design, produce, and implement efficient security tools and measures of protection and reaction to support availability, integrity and confidentiality of ICT infrastructures and services.

[9] www.oecd.org/dataoecd/16/22/15582260.pdf – See Annex F to this Guide.

The private sector has a major role to play by providing users with security technologies that should be cost effective, user friendly, transparent, auditable and third party controllable.

Security solutions must satisfy basic security criteria such as **availability, integrity and confidentiality (the AIC criteria)** (Figure 1.7). Other criteria that are often cited in this context are: (i) **authentication**, which makes it possible to verify the identity of an entity; (ii) **non-repudiation**; and (iii) **imputability**, which make it possible to verify that actions or events have taken place and to attest who is responsible for them.

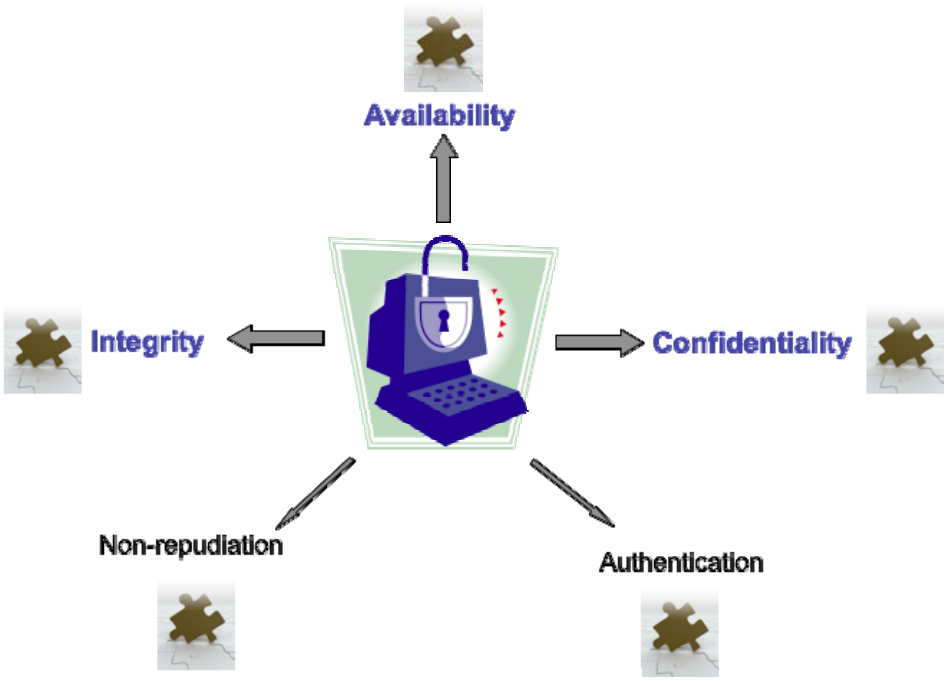

Figure I.7: Basic ICT security criteria

To ensure the **availability** of services, systems and data, the components of the infrastructure systems must be appropriately sized and possess the necessary redundancy. In addition, operational management of resources and services must be provided.

Availability is measured over the period of time during which the service provided is operational. The potential volume of work that can be handled during the period of availability of the service determines the capacity of the resource (a server or network, for example). The availability of a resource is closely linked to its accessibility.

Preserving the **integrity** of data, processing or services means protecting them against accidental and intentional modification, tampering and destruction. This is needed to ensure they remain correct and reliable. To prevent tampering, there needs to be a way of certifying that they have not been modified during storage or transfer.

Data integrity can only be guaranteed if data are protected from active tapping techniques that can be used to modify the intercepted information. This type of protection can be provided with security mechanisms such as:

- Strictly enforced access control;
- Data encryption;

- Protection against malwares (viruses, worms and Trojan horses, etc.).

Confidentiality is the safeguarding of the secrecy of information, information flows, transactions, services or actions performed in cyberspace. It guarantees the protection of resources against unauthorized disclosure. Confidentiality can be implemented by means of access control and encryption.

Encryption helps to protect the confidentiality of information during transmission or storage, by turning it into a form that is unintelligible to anyone who does not possess the means to decrypt it.

The purpose of **authentication** is to remove any uncertainty about the identity of a resource. It presupposes that all entities (hardware, software and persons) have been correctly identified, and that certain characteristics can serve as proof of identification for them. In particular, logic-based access control systems to ICT resources require that the **identification** and authentication of entities be managed.

Identification and authentication procedures are implemented in order to help achieve the following:

- **Data confidentiality and integrity**: access to resources is restricted to identified authorized users, and resources are protected against change by all except those who are so authorized;
- **Non-repudiation and imputability**: actions can be traced to an identified and authenticated entity;
- **Traceability of messages and transactions**: transmissions can be traced to an identified and authenticated entity;
- **Proof of destination**: the message can be proven to be addressed to an identified and authenticated entity.

In some circumstances, it is necessary to verify that an event or transaction has taken place. **Non-repudiation** is associated with the concepts of **accountability**, **imputability**, **traceability** and, in some cases, **auditability**.

Establishing responsibility presupposes the existence of mechanisms for authenticating individuals and attributing their actions. The possibility of recording information to make it possible to trace the performance of an action becomes important when there is a need to reconstitute the sequence of events. This is particularly important for performing computer investigations to find a system address used to, for example, send data. The investigators need to be able to save the information that is to be used to conduct subsequent analysis for system auditing purposes (information logging). This is called system auditability.

I.5.5 Social dimension

The state needs to ensure that all participants in the Internet are aware of the basic steps required to strengthen the level of security. It needs to implement *information campaigns* and *civic education* for a responsible information society, covering the challenges, the risks and the preventive and deterrent security measures. The *security culture* must be embedded within an ICT culture.

From a citizen point of view, cybersecurity issues should focus on: (i) the protection of individuals; (ii) the protection of private data; (iii) the respect of basic human rights; (iv) the quality e-services; (v) the confidence into ICT infrastructures and applications. From the individual point of view, cybersecurity should not be restricted to homeland security. Nowadays, a trend is emerging concerning the evolution of the way to apprehend the concept of information security or cybersecurity. This trend is towards a much more badly defined and complex terminology relating to critical information infrastructures protection. This modification of terminology without a real definition, introduces more complexity, and could lead to an overemphasis in cybersecurity on critical information infrastructure protection and homeland security.

Any citizen should:

- Understand threats for the end-user (virus, spam, identity usurpation, fraud, swindle, privacy offence, etc…) and their impacts;
- Understand how to adopt a security behaviour for a safe use of ICT resources;
- Understand how to build a global cybersecurity culture based on well recognized international standards and recommendations, involving several kinds of stakeholders.

So many open questions remain concerning ICT security. These questions go beyond the purely technological dimension of Internet and its security. *Transparent and controllable security solutions* associated with universal know-how will contribute toward building an *inclusive information society* in regard to *democratic principles*, *basic human rights*, and the *sovereignty of states*. The Internet should be made into a commons open to all, without taking excessive security risks. Collectively, all players in cyberspace need to develop, consent to, and respect a uniform code of security ethics.

The *virtual nature of the Internet*, and its recreational aspects, can blind users - especially young persons and novices - to its considerable capacity to do harm. The consequences can be devastating for organizations and individuals who fall prey. Controlling technological risks means more than hunting down hackers or setting up technological barriers. The most serious consequences are sometimes due to: (i) sheer negligence resulting from incompetence; (ii) misconceived or poorly implemented technology; (iii) excessive authority for system administrators; or (iv) mismanagement.

PART II

CYBER TREATS, CYBER ATTACKS AND CYBERCRIME ISSUES

Part II presents cyberthreats, cyberattacks and cybercrime issues in order to be able to answer the following questions:

- What is cybercrime?
- Why and how is cybercrime possible?
- Why is it important for developing countries to overcome cybercrime and cybersecurity issues?
- How could developing countries fight against cybercrime?

A comprehensive approach is proposed to understanding the issue of cyberthreats and cyberattacks, and cybercrime is defined and illustrated to help developing countries get prepared to face the issues and challenges linked to cybercrime and to the deployment of information and communication technologies (ICT).

Part II also presents:

- The basicsof telecommunication networks and Internet technologies in order to understand how cyberthreats can become a reality;
- Sources of vulnerability of the Internet;
- The types, tools and operation of cyberattacks; and
- Examples of misues of ICT and different expressions and examples of computer-related crime and cybercrime. Most cybercrimes are illustrated by real cases of attacks, in order to better understand what cybercrime is. These examples of cybercrime cases, taken mostly from developing countries where the Internet is already widely used and this type of crime is well reported, have been anonymized.

Most cybercrimes are illustrated by real cases of attacks, in order to better understand what cybercrime is. Examples are not exhaustive and do not intend to point out any weaknesses or denunciate those that have been victims of cybercrime and do not constitute an incitation to commit such crime. Based on real cybercrime cases, taken mostly from developing countries where the Internet is already widely used and this type of crime is well reported. Examples have been transformed to become anonymous. This does not mean that other countries are not subject to cybercrime, or that other examples do not exist. Examples have been written with the collaboration of Mrs Amélie Magnin.

II.1 UNDERSTANDING INTERNET TECHNOLOGIES

II.1.1 Telecommunication infrastructure and e-services

Internet network access points have proliferated in recent years. Cybercafés are still on the increase. More and more countries are building a more accessible *information transport infrastructure* offering even greater capabilities.

In addition to *fixed telecommunication infrastructures*, there has been an emergence of *wireless infrastructures*, which allow *user mobility*. Satellite and space infrastructures and terrestrial radio systems support wireless technologies. Mobile telephony has become a means of providing services in many developing countries.

On several continents, the GSM (**Global System for Mobile Communication**) standard has been established for the transmission of voice, and sometimes for small volumes of data. However, it is the new generation of mobile networks that is paving the way for more extensive use of mobile multimedia handsets. These new networks are based on the UMTS (**Universal Mobile Telecommunication System**) standard, which offers better transmission capabilities than GSM. At the same time, GSM networks continue to evolve – they are incorporating GPRS (General Packet Radio Service), which allows increased transmission speeds that can meet the requirements of data applications over mobile networks.

The sudden arrival of technologies like GSM and UMTS reflects not only technological, but also *behavioural and economic changes*. The telecommunication market was once the exclusive province of operators. Mobile communications is now a booming industry, within a context of fierce global competition. It has allowed a new service, radiotelephony, to enter the telecommunication market, and is constructing an infrastructure that can be reused for all kinds of data transfer and services.

Telecommunication infrastructure refers to all the transmission media on which communication services can be set up. It is important to draw a distinction here between (i) the transmission channels and routing technologies, and (ii) the telecommunication solutions and services offered to customers. It is thus possible for companies that do not own a particular infrastructure to nevertheless utilize that infrastructure as a transport facility for providing particular applications.

With the widespread availability of **multimedia equipment** and **high-performance communication infrastructures**, as well as the convergence of the audiovisual, information technologies and telecommunication worlds, the concept of a fully digital information chain emerges (**digital convergence**). The concept of **information highway** encompasses the widespread provision, over high−performance communication infrastructures, of a range of public or commercial services, in areas such as health, education, culture, land planning, administration and media for example.

Irrespective of the technology adopted for the deployment of **e−services**, telecommunication infrastructures in the developing countries should provide for the following:

- Standardized digital internetworking (voice, data, and image) of a defined set of basic services that are easy to set up and maintain. They must supply the requisite geographical national and international coverage within the framework of a total−quality approach and optimum cybersecurity. This means a **sustainable**, stable and granular offering that can be altered at little technical and economic cost.
- Technical and commercial harmonization and protection against possible cartelization. This means a harmonious development of infrastructures and services, with a guarantee of active regulation of abuses of dominant positions.

II.2 FUNDAMENTAL PRINCIPLES IN TELECOMMUNICATION AND NETWORKING

II.2.1 Several types of networks

A telecommunication network consists of a set of **information and transmission resources** working together to provide various **communication services**. These services include remote access to distributed resources, transfer of information and remote execution of programs.

In today's world, all economic activity is critically dependent on the availability of an efficient communication infrastructure that can link all sorts of equipment, applications and people, irrespective of distance, place and the type of information flows to be transferred.

Networks are distinguished primarily according to a number of criteria. These include (i) geographical coverage, topology[10], (ii) technology employed and applications supported, (iii) mode of operation, (iv) type of transmission medium (wire line or wireless), and (v) private-owned or public-owned.

Historically, the first networks were *wide area networks*[11] – telephone, telex, Internet, etc. It is with the dawn of PCs at the beginning of the 1980s that local area networks emerged[12].

These distinctions have tended to become less marked of late, since the networks in question are interconnected. For example, a *local area network* (LAN) may be connected to other LANs, and thereby become a larger network. Moreover, networks are no longer restricted to supporting a single type of application, but can be used to transmit voice, data and video images: they have become multimedia networks.

A private network is one that belongs to an organization that has exclusive usage rights. A *public network* is one in which telecommunication services are made available to various individuals or institutions on the basis of particular subscription arrangements.

The main transmission technologies used to set up wide area networks are TCP/IP[13]. In the business LAN market, the main technology is Ethernet and its high-speed variants, fast Ethernet and switched Ethernet. Optical transport technology constituted a major step in the evolution of transmission infrastructures and arteries, enabling high-speed and high-quality transmission, dynamic bandwidth allocation, variable bit rates and multi-usage.

II.2.2 Network components

Transmission media are required in order to connect computers and create a network. These may be physical media, such as twisted cable pairs, coaxial cables, or optical fibre. They may be intangible media, such as radio and infra-red waves. These different media each have specific characteristics that determine their reliability and capacity to carry varying amounts of information at different speeds.

The transmission or capacity of an interconnection medium is the quantity of information it can transfer during a given lapse of time. It is expressed in kilo, mega or even terabits per second (e.g. 100 Mbit/s). It is proportional to the bandwidth of the transmission medium. The **bandwidth** designates the range of frequencies that can pass through the medium without modification.

---

[10] A network's topology is the pattern of links connecting its different elements or nodes.

[11] A wide area network or WAN is one that connects computers spread over a relatively large geographical territory (> 100 km), or even worldwide.

[12] A local area network (LAN) it is one that connects computers in a small geographical area, a few kilometres in size (~10 km). A metropolitan area network (MAN) is one that interconnects local networks that may belong to different entities, having a geographical coverage of up to 100 km. Telecommunication specialists are coining new terms to identify different types of networked resources or to depict specific application domains. For example, the following acronyms are encountered in specialized texts: (i) HAN (home area network), a network interconnecting remotely controllable equipment such as an oven, VCR, or lighting and heating equipment within a house; (ii) CAN (car area network); (iii) SAN (storage area network); etc.

[13] TCP/IP: Transmission Control Protocol / Internet Protocol.

A *network interface*, resolves **connectivity** issues. It adjusts the signal transmitted or received by the computer so that it can be transmitted over a specific medium and network. An example of a network interface between a computer and a transmission medium is a modem (modulator/demodulator). In theory, any electronic component can be connected to the network insofar as it has an appropriate hardware and software connection interface.

A *network's transport infrastructure* consists of, (i) user systems that serve to access a network, (ii) computers that manage and process applications (data hosts and servers), and (iii) communication processors. The latter are computers that carry out one or more functions required to manage and set up telecommunications. Those functions include, (i) resource optimization and sharing, (ii) routing of data, (iii) management of addresses and names, and (iv) interconnection. Examples of communication processors are routers, multiplexers, concentrators, switches, and interconnection gateways.

In order for communication to take place, information must be transmitted reliably according to exchange arrangements that are satisfactory for the correspondents. Systems interconnected over telecommunication networks are *a priori* different. In order to be able to dialogue, they must use the same frame of reference for communication. In other words, they must speak the same language and follow common exchange rules. Networked computers must comply with identical *communication protocols* and follow the same dialogue rules in order to be able to communicate. These protocols are integrated in the communication software.

A *de facto* standard is one that unofficially becomes a market reference due to wide-spread common use. For example, all the protocols stemming from the Internet community are *de facto* standards. Frequently, a *de facto* standard will eventually receive official sanction from a universally recognized organization.

II.3 INTERNET: A NETWORK OF NETWORKS

II.3.1 Network access

The Internet started in the US several decades ago and spread progressively by linking together neighbouring information systems and computer networks. This reticular development is still ongoing. It determines the structure of the network, which is a *network of networks*. The speed of this development, the technical complexity of managing these environments, and the sheer number of different actors, make it difficult to implement efficient global means of protection. This difficulty is exacerbated by the fact that data is exchanged through external communication environments, whose control is completely beyond the power of the organizations that use them.

In hardware terms, the Internet, like any telecommunication network, comprises information systems, connection elements and transmission media. The information systems include (i) those which are used to access the network and allow dialogue with the end user (PCs, mobile phones, pagers, PDAs, etc.); (ii) those that support applications (web servers, database servers, etc.); and (iii) those dedicated to processing within the network (routers, interconnection gateways, etc.) and to manage system and network.

Data is exchanged between computers over the transmission media by which they are physically connected. **Mobile Internet** is when the access point to the Internet infrastructure is through system allowing user mobility, such as a mobile phone.

The communication protocols of the TCP/IP family enable data transfer, routing and communication between the distributed information processes and human users. These softwares are standardized in the Internet world. They constitute a communication interface that enables interoperability of different types of systems. To communicate in the Internet environment, a computer must be equipped with these communication protocols and have an IP address affording it a unique identity (Figure II.1).

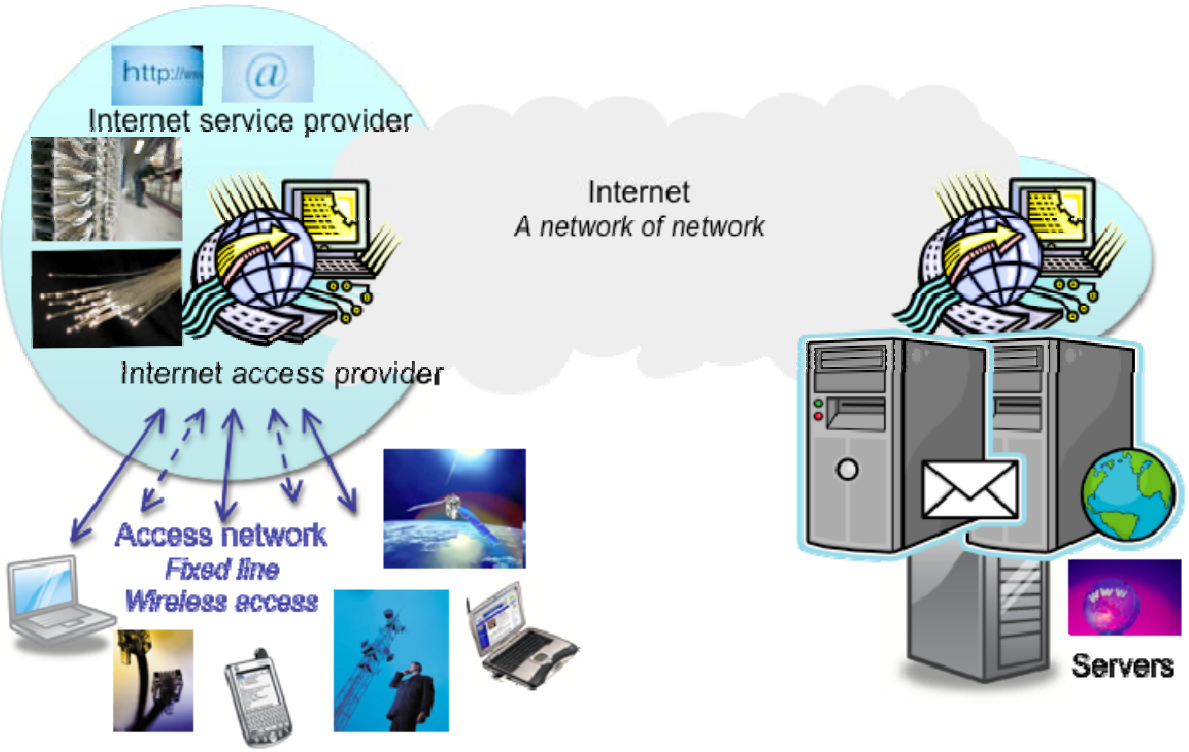

Figure II.1: Accessing the Internet

Internet designates the whole of the communication infrastructure made available to the public in order to communicate. When an organization wishes to use this infrastructure privately and restrictively, it can establish a **virtual private network** (VPN) over the Internet. For internal needs, it may use Internet technologies to construct a private network or **intranet**. When the intranet is also open to a number of partners (customers, suppliers, etc.), it is called an *extranet* (Figure II.2).

Together with e-mail, the **World Wide Web** (or "web", for short) is the most important Internet application. A multitude of services have been developed on the basis of web navigation. It is possible to navigate throughout the web, thanks to client software (*browser*), which is installed in the user's workstation. The browser allows remote access to *web servers*. It can be used to search, consult or transmit information, or even to run programs. The notion of browsing or surfing the web stems from the fact that documents (*hyperdocuments*) have been designed, structured and formatted so as to be read in a non-sequential manner, using tags and navigation links that were inserted when they were created. Activating a link takes the reader to another part of the document or to a different document, possibly located on a remote computer. One surfs from site to site by activating these hyperlinks.

The *Web* (*World Wide Web*, *W3*), along with electronic mail, is the Internet's most significant application. The number of services developed on web navigation facility is infinite.

The Internet is used for private and professional issues, from the simple exchange of data to strategic business or governmental applications.

Figure II.2: Internet – intranet – extranet

II.3.2 IP address and domain name

Access to the Internet network is attained through access points managed and controlled by specialized enterprises called **Internet Access Provider** (IAP) or **Internet Service Providers** (ISP). Each IAP / ISP is itself connected to the Internet over permanent telecommunication lines that it shares among its different clients. In addition to this basic service, an Internet Service Provider generally offers an e-mail management service and can also host its clients' websites for example.

In order to communicate over the Internet, one needs an Internet address (**IP address**). In the most current release of the Internet Protocol (IPv4) it is a 32 bits binary sequence unambiguously identifying each machine communicating on the Internet[14].

Since it is impossible to memorize such number sequences, even the decimal ones, *names* (often mnemonic) or logical addresses are used to identify resources in the Internet environment. These IP addresses and corresponding names are stored and managed in electronic directories called **name servers**, which are known in practice by the acronym DNS (**Domain Name Server**).

To implement communications in an open environment, it is necessary to be able to allocate a unique identifier in a given *naming domain*. The parties involved in the communication have to be identifiable (addresses, systems, application processes, entities, management objects, etc.), as must the implementation tools for setting up the communication (protocols). In order to ensure unique names worldwide, there are procedures for *registering names* with competent *authorities*, whose role is to allocate an unambiguous and unique identifier to each entity or object.

Generic Internet domain names are registered in this logical registration structure. The relevant part of the registration tree in this case is the root node of the highest−level domain names, which are

[14] An IP address is unique. It can be allocated permanently (*static IP address*) or not (*dynamic IP address*). An IP address is expressed in its decimal form. It is comprised of four decimal numbers separated by marks (point). For example, the address 128.10.2.30 corresponds to the binary value 10000000.00001010.00000010.00011110.

called **top−level domains** (TLD). These primarily identify countries, indicated by two letters (.dz for Algeria; .ke for Kenya; .pe for Peru; .pk for Pakistan; .zw for Zimbabwe; etc.). Functional domains such as .int are used to identify international entities (www.itu.int); .com identifies commercial organizations; .org identifies organizations; and .biz identifies the business world. The following are examples of functional domains:

- .com commercial organizations;
- .edu academic institutions in North America;
- .org organizations, institutional or otherwise;
- .gov American government;
- .mil American military organizations;
- .net network operators;
- .int international entities;
- .biz for the business world;
- .info for all uses;
- .name for individuals;
- .museum for establishments in which collections of objects are kept and classified for conservation and exhibiting to the public;
- .aero for the air-transport industry;
- .coop for cooperatives;
- .pro for professions;
- Etc.

Within these broad domain designations, there are sub-domains, corresponding to large corporations or important institutions.

Internet Corporation for Assigned Names And Numbers (ICANN)[15] is responsible for allocating names and addresses and must ensure that they are all unique. This responsibility for managing names may be delegated to a sub-domain that is hierarchically under its authority. For example, in the case of France, the registration authority (accredited registrar directory) accredited by ICANN is AFNIC[16].

According to ICANN: "The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for internet protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) top-level domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA)[17] and other entities. ICANN now performs the IANA function."

The authority for the allocation and management of addresses was entrusted exclusively to an American association, on American territory, operating under American law.

ICANN, is a not-for-profit, multi-stakeholder organization, based in California, dedicated to coordinating the Internet's addressing system, has now taken over the IANA function in 1998, where US representation remains overwhelmingly dominant. By its function, ICANN “potentially controls” access to the Internet. This poses for any Internet actor a genuine problem of dependency.

---

[15] http://www.icann.org/index.html.

[16] http://www.afnic.fr.

[17] http://www.iana.org/

The **Internet Governance Forum** (IGF), an international forum for multi-stakeholder policy dialogue (founded in 2006 following WSIS-Tunis commitment[18]) addresses the need for more international participation in discussion for Internet governance issues[19].

Organizations cannot control or govern the criterion of security in terms of the availability of infrastructures, services, and data, in cyberspace because they depend, for their access to the Internet, on the allocation of IP addresses and domain names - hence, on outside entities.

It is vital that the addresses, processes and systems involved in the management of names and addresses, and the routing of data, should be characterized by availability, integrity, reliability and security. It is the responsibility of the entities in charge of transport infrastructures to protect and effectively manage their communication environments.

The domain name directories can be seen as databases managed by DNS servers. ICANN coordinates some fifteen DNS root servers, the vast majority of which are located in North America. ICANN manages the top-level domain names and IP addresses. This includes all of the domains referred to above (.org, .com, etc.), as well as the 244 domain names for the different countries (.cn – China, .ga – Gabon, .lk – Sri Lanka, .pf – French Polynesia, etc.). Local DNS servers called **resolvers** keep a copy of the information contained in the root servers. These resolvers, frequently associated with strategic network access points or linked to Internet Service Providers, serve to answer user queries regarding the translation of a domain name into an IP address (Figure II.3)[20].

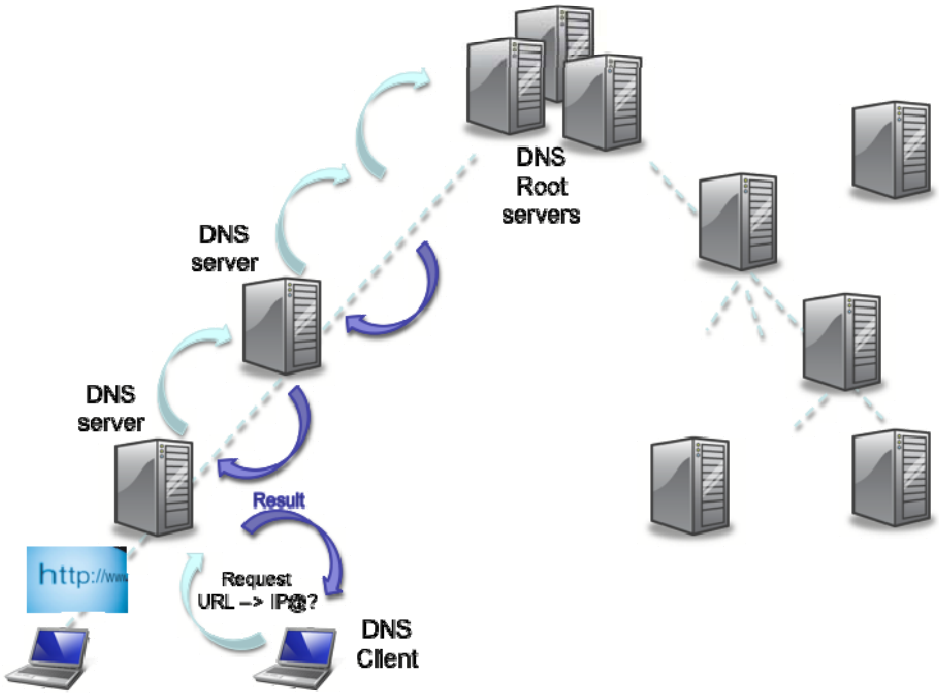

Figure II.3: DNS server tree structure

[18] World Summit on the Information Society Tunis commitment 2005. - http://www.itu.int/wsis/docs2/tunis/off/7.html
[19] http://www.intgovforum.org/cms/

[20] Figure adapted from: "*Sécurité informatique et télécoms: cours et exercices corrigés*"; S. Ghernaouti-Hélie; Dunod 2006.

II.3.3 IP & TCP/IP protocols

Version 4 of the **Internet Protocol** (IPv4)[21], which has existed since the beginnings of the Internet network, is still widely used. The role of this protocol is to *encapsulate the data* to be transmitted, in order to constitute **IP packets** that will be routed over the Internet network to their destination. Each packet contains, among other things, the IP address of the sender system (source) and the IP address of the destination system. Routing is carried out by handing on to each intermediate system (router) crossed, following the interpretation of the packet addresses and the routers' routing algorithm.

The IPv4 protocol does not include any function or mechanism for guaranteeing secure service. Indeed, under IPv4, there is no way of authenticating the source or the destination of a packet, nor of ensuring the confidentiality of the data transported or of the IP addresses involved in the transfer of information between two entities. In addition, since the protocol operates in connectionless mode, there is no guarantee of any of the following:

- Delivery of data (possible data loss);
- Delivery of data to the right addressee;
- Correct sequencing of IP packets belonging to the same application.

The IP protocol offers an *unreliable IP packet delivery service*. It operates in so-called "*best effort*" mode. In other words, it does its best under the circumstances and does not guarantee packet delivery. In fact, it does not guarantee any quality of service whatsoever, and there is no error recovery. Thus, a packet can be lost, altered, duplicated, fabricated (forged) or delivered out of sequence without the sender's or recipient's knowledge. Because no prior logical relationship is set up between sender and recipient, this means that the sender sends his packets without informing the recipient and they can get lost, take different routes, or arrive in the wrong order.

To counter this lack of quality of service, the **Transmission Control Protocol** (TCP) is installed in end systems. TCP offers a reliable transport service in connection−oriented mode. However, the TCP protocol does not offer any security service in the true sense of the word.

On this transport “TCP/IP” communication protocol infrastructure, application protocols have been implemented to support distributed applications. Various communication protocols have been established, primarily to meet communication needs. These include: (i) **SMTP (Simple Mall Transfer Protocol)** for e-mail services; (ii) **FTP (File Transfer Protocol)** for the transmission of files; and (iii) **HTTP (HyperText Transfer Protocol)** for Internet navigation (Figure II.4). None of them support or offer security services in native mode.

[21] IPv4: RFC 0791 –www.ietf.org/rfc/rfc0791.txt IPv4 and main TCP/IP protocols:
TCP: RFC 0793 – www.ietf.org/rfc/rfc0793.txt – UDP: RFC 0768 – www.ietf.org/rfc/rfc0768.txt – FTP: RFC 0959 – www.ietf.org/rfc/rfc0959.txt – HTTP version 1.1: RFC 2616 – www.ietf.org/rfc/rfc2616.txt – Telnet: RFC 0854 – www.ietf.org/rfc/rfc0854.txt

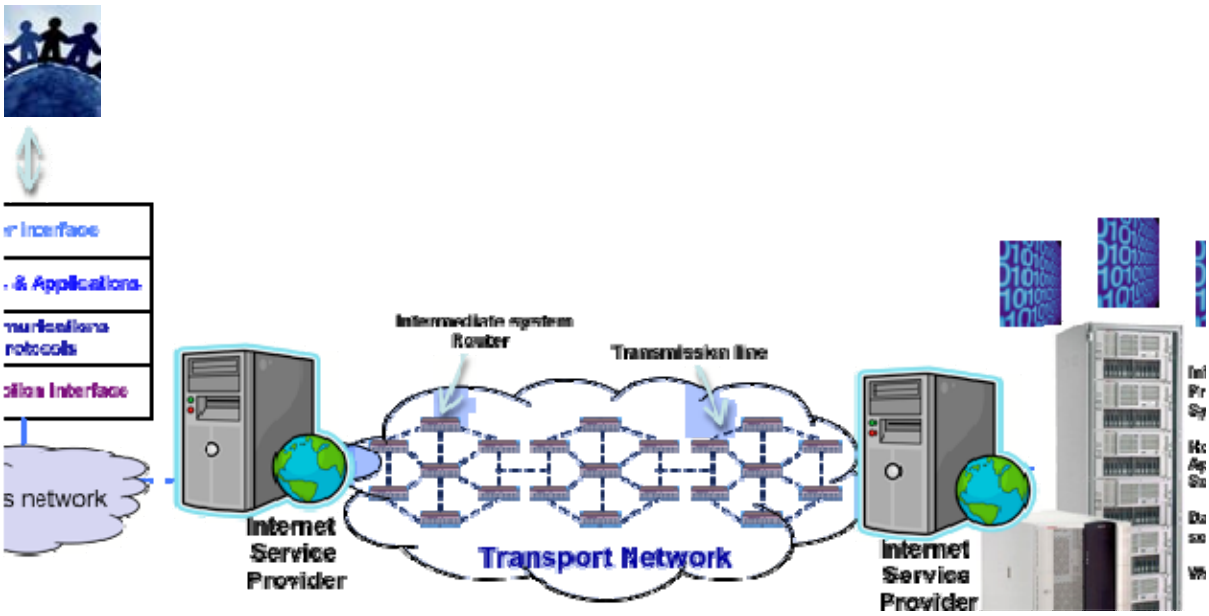

Figure II.4: Internet communication protocols

II.3.4 Vulnerabilities of the Internet

Figure II.5 identifies the sources of vulnerability for an Internet infrastructure. These include natural disasters, errors and malevolence. Threats may come from a lack of control of the configurations, or from fraudulent exploitation of vulnerabilities of interconnected systems - hardware, software and administration weaknesses. Furthermore, network administration tools, such as monitoring or remote configuration tools, can be used with malicious intent.

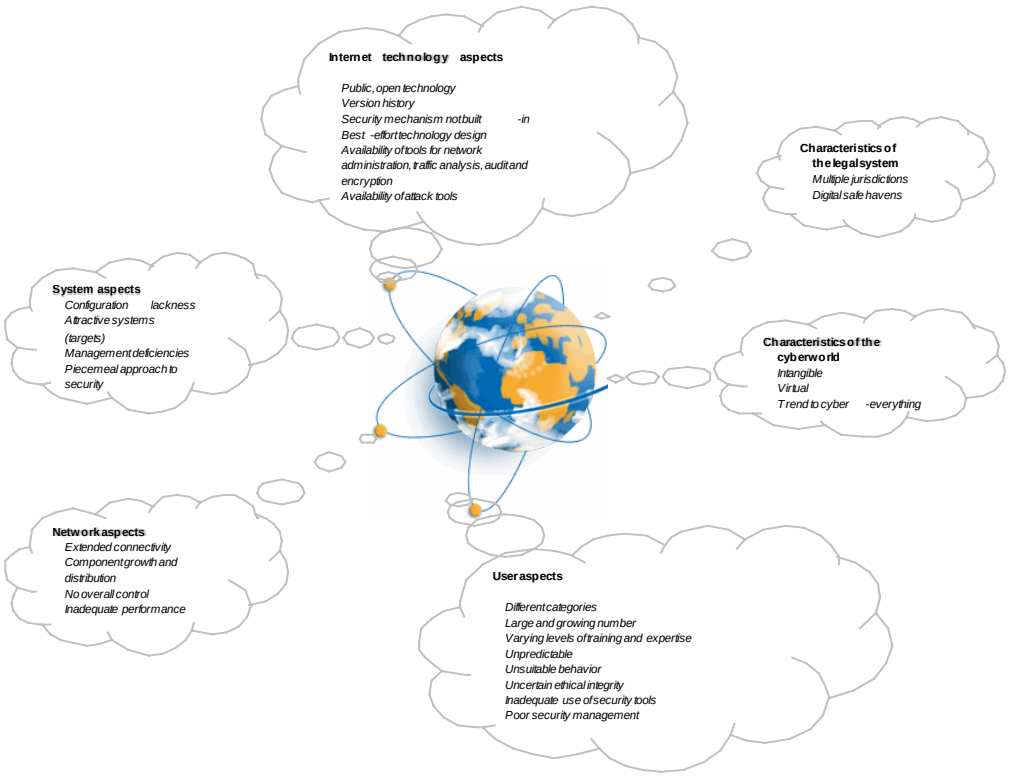

Figure II.5: Sources of vulnerability for the Internet

The technical specifications and operating modes of the Internet belong to the public domain. Anyone can adopt these network technologies to perform communication services - or divert them for malevolent purposes. In addition, most Internet protocols have been designed without integrating security mechanisms. The best example is the protocol that is the cornerstone of the Internet infrastructure: IPv4. All TCP/IP protocols and Internet services can be corrupted and used for malicious acts, such as service disruption, data and resource theft, modification, and destruction.

II.4 CYBERATTACKS

II.4.1 Passive and active attacks

There are various ways for criminals to exploit Internet weaknesses – there are a number of different types of attacks. Law enforcement officials make a distinction between passive and active attacks (Figure II.6).

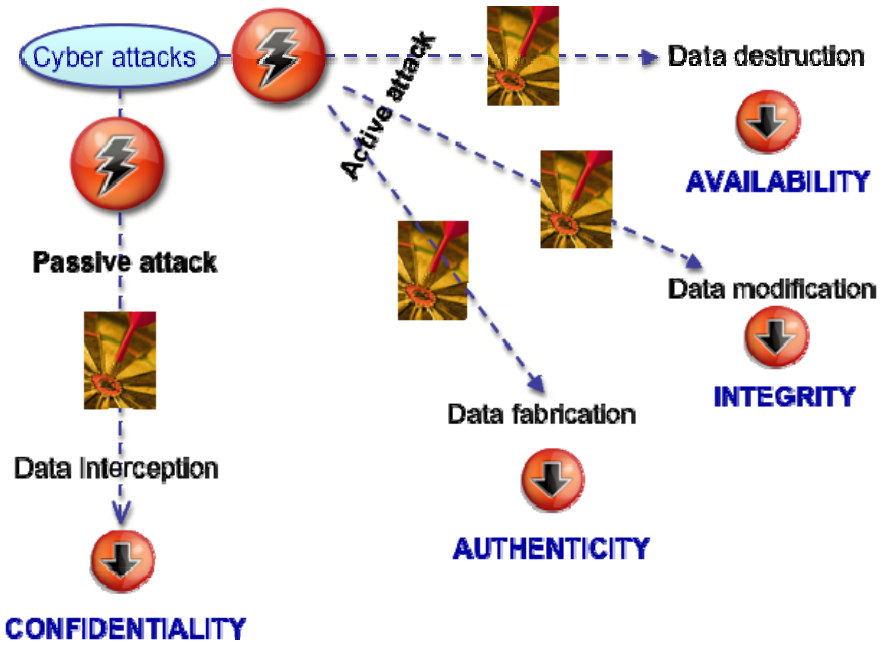

Figure II.6: Passive and active attacks

II.4.2 Denial-of-Service attacks

A **denial-of-service (DoS) attack** is typically carried out by overloading system capacity, and preventing legitimate users from accessing and using the targeted resource. The system, submerged with far more requests than it can cope with, crashes and becomes unavailable. A denial-of-service attack aims to disrupt operations. It represents a particularly dangerous threat for organizations that rely almost entirely on the Internet for business and communication.

Malevolent can perpetrate DoS attacks by taking advantage of flaws in the operating system and exploiting certain system features, such as buffer management. The latter is called a **buffer overflow attack.** DoS attacks cause serious malfunctioning that can lead to system shutdown (Figure II.7).

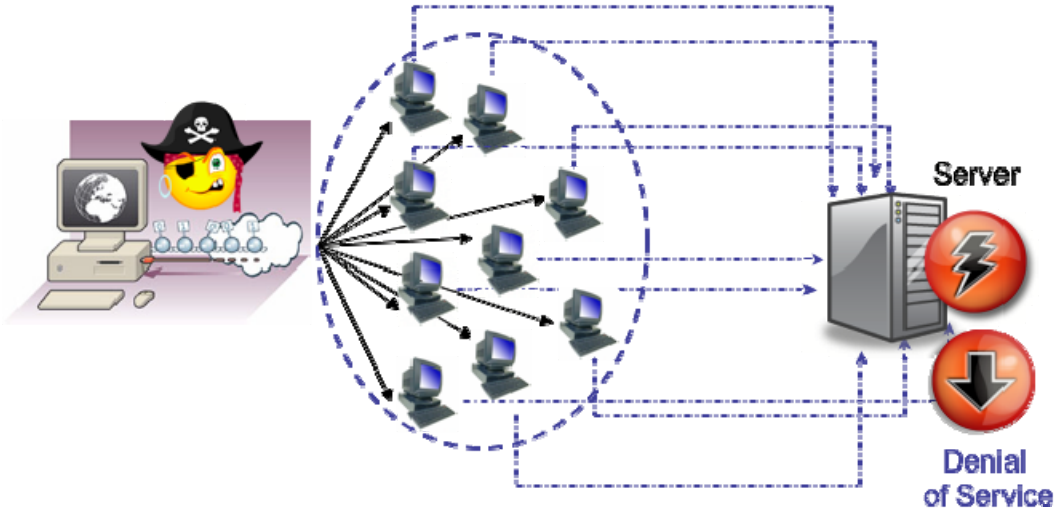

Figure II.7: Denial-of-service attack

DoS tools are designed to send many request packets to a targeted Internet server - usually a web, FTP, or mail server - in order to flood the server's resources and thus render the system unusable. One form of a DoS attack is called **e-mail bombing**. This is done by flooding a user's inbox with messages. Any resources connected to the Internet are vulnerable to DoS attacks.

Example:

A hacker attacked an authentication server of a National Pharmacists Association, resulting in downtime of all services. Five thousand users were no longer able to access the website, and medicine Internet trading services were interrupted. The hacker launched a DoS attack that consisted of bombarding the authentication server with many unauthorized attempts. The hacker used the Internet to find hacking tools as cracker software, through forums and hacking sites. He intercepted the password of the administrator of the National Pharmacists Association. The hacker used this stolen identification to gain access to protected documents that contained confidential information. In addition, the fraudster found 80 other identifications and installed a password cracker tool directly on the server to find user's passwords. This new attack caused more disruption of service, with bad financial consequences for the association.

There are three basic ways to attempt a DoS attack: (i) by the consumption of all resources, such as bandwidth, preventing legitimate traffic; (ii) by the destruction or alteration of configuration information; and (iii) by the disruption of physical network components to deny access to a service.

The consumption of scarce resources is a tool often used to launch DoS attacks. The main goal of attackers is often to disrupt the network connectivity in order to prevent hosts from communicating. For example, in the **SYN**[22] **flooding attack**, the attacker sends a large number of requests to open a TCP connection. Upon receiving the SYN packet, the server allocates the necessary memory for the connection and enters it in a queue of half-open connections. The attacker will never answer and the server can no longer accept new, legitimate connections once the queue overflows. Therefore, the network connectivity is disrupted. Moreover, the attacker can remain anonymous - he does not wish in any case to open authentic connections. Indeed, he can forge the source address of his SYN packets to hide his identity.

Bandwidth is also viewed as a scarce resource. An attacker can consume bandwidth by generating a large number of packets directed to the network. This method, called a **smurf attack**, aims to drown the target with the help of traffic amplifiers[23]. The **disruption of configuration** systems relies on the possibility that a computer is badly configured. One example would be for the change of the routing information in the routers to lead to the **network's breakdown**.

An organization has to secure all network components physically. Access to computers, routers, power stations and critical elements should be restricted to legitimate persons. The destruction of cooling stations can result in the overheating of some electronic devices and the disruption of a whole network.

A **distributed denial-of-service (DDoS) attack** uses a large number of computers infected by a worm or a Trojan horse to launch simultaneous attacks on a target in a very short time. A remotely controlled infected computer is called a "zombie" . Zombie computers can for example, bombard the system with thousands of e-mails, causing denial-of-service at the mail server - and thereby deny the service to legitimate users.

Example:

[22] SYN: Synchronization

[23] The attacker sends a large amount of ICMP echo-request (ping) to IP broadcast addresses, with the target address as the source address. The network then serves as a smurf amplifier. The "pinged" machines send their response to the intended victim. On a multi-access broadcast network, hundreds of machines might reply to each request. The use of spoofed broadcast ping messages floods the target system.

A national police force caught a young boy and charged him with launching for sport DDoS attacks on websites managed by a particular company. The hacker took advantage of his administrative position on an online music forum to hide malicious code in the website. Users of the music forum unknowingly downloaded the malicious software, which subsequently gathered information about the users. The hacker used these infected computers as zombie relays, to launch DoS cyberattacks.

DoS and DDoS attacks are intended to cripple system resources. They typically operate by overloading a server with requests for the ordinary services it is designed to provide routinely, thereby preventing it from delivering the service to regular users. These requests resemble ordinary requests. It is the sheer volume of requests that overwhelms the system. This makes it so that a DoS or DDoS attack is very difficult to identify and to prevent.

II.4.3 Defacement attacks

A **defacement attack** is carried out by replacing the victim's web page with a **forgery**, where the content of the forged page (e.g. pornographic, political), will depend on the criminal's motives.

One variation of this type of attack involves redirecting users to a decoy website that looks exactly the same as the one they were accessing. Once those users have entered the phoney site they are asked to disclose sensitive information such as a credit card number. This approach is used in **phishing attacks**.

Example

There have been a number of cases in which fraudulent websites imitated legitimate websites of well-known banking institutions. These websites would use a domain name such as www.trustedbank.com. They would claim that the website was operated by a company with a name such as "TrustedBankForCountryQ". They would claim that this company offered various banking services in a well-known financial place. But, in truth, this TrustedBank would be a completely fraudulent entity.

A criminal can deface the content of websites for purposes of **disinformation**. Its motivation might be: (i) to influence events; (ii) to manipulate the stock exchange; (iii) to spread uncertainty or fear; or (iv) to manipulate public opinion. These can be viewed as **semantic attacks**. They subvert the meaning of the information content, and fall into the category of **infowar**.

An attacker can gain access to a web server – indeed, to the whole private network - by exploiting vulnerabilities in web application or technical and managerial errors. If they are not well protected, Web-based applications are vulnerable and expose the whole information system of an organization to cyber attacks.

II.4.4 Malware attacks

A malicious code (or *malware*) is any program that can deliberately and unexpectedly interfere with the normal operation of a computer. Usually, malware programs have been designed to obtain financial gain.

The number of malware attacks continues to grow has become veritable pandemics. They have become ubiquitous, affecting anyone in any sector of activity. No system, whether it is a desktop, laptop or a mobile phone, is immune. *No hardware or software platform is immune* and malicious code for mobile devices also exist. New mobile phones contain a great deal of user-installable software, this represents new sources of vulnerability and therefore, new opportunities to install programs that can have a negative impact on security.

The mechanisms used to propagate malware from one system to another vary. Different vectors used to spread malicious codes are: (i) peer-to-peer file-sharing networks; (ii) remotely exploitable vulnerabilities; (iii) IRC (Internet Chat Relay), and (iv) IM (Instant Messaging). Any action such as downloading files with viruses from peer-to-peer networks, opening an e-mail with a worm

attachment, or surfing on a website dropping a Trojan, can lead to infection by and propagation of the malware.

Malware includes the following kinds of software:

- **Downloaders**, which are used to download and install data and programs remotely;
- **Keyloggers**, which monitor which keystrokes the user enters; there are also hardware keyloggers, invisible at the software level, that record data;
- **Zombies or "bots"** (short for "*robots*"), which are programs that allow the system to be controlled remotely for the purpose of building a hidden army of computers. They are used for spamming purposes, phishing attacks, or for the distribution of adware:
- **Adware** (advertising software), which are used to customize business transactions;
- **Spyware**, which are used to clandestinely record information;
- **Viruses** and related products, such as worms, Trojan horses, and logic bombs.

The generic term "virus" is used to designate any *harmful computer program* capable of reproducing and propagating itself. A virus can cause infection, destruction, or misappropriation of resources. Viruses can be distinguished on the basis of their signature, behavior, how they replicate and spread, or the types of malfunctions they induce. The purpose of a computer virus, like that of its biological counterpart, is to reproduce and propagate itself from computer to computer. The damage that viruses cause to the integrity of the contaminated information resources may range from mild annoyances to major destruction, with an impact on system availability and confidentiality. The main effects are loss of data, loss of working time, loss of public image, and loss of confidentiality.

Example

A virus hits a country Stock Exchange system and causes a complete disruption of service. The virus first infects a computer connected to the trading testing system and launches a DoS attack. It generates a large amount of false traffic, causing an overload of the routers and finally disrupting communication services. All data being entered in the system is not taken into consideration. The investigation claims that no data has been stolen. However, the damage may not be limited to the service disruption of the markets, as this sort of accident can also harm the credibility of the institutions attacked.

Most often viruses exploit security holes in operating system platforms and are installed in a system without the user's knowledge and the computer is infected as soon as a system platform runs the malicious code. A virus attacks its environment and contaminates other environments with which it comes into contact. The normal way for viruses to propagate and execute is to await inadvertent activation by the user - for example, by the user starting an infected program. Most viruses are propagated via e-mail attachments. Clicking on the file icon or downloading the file commonly activates them. The means by which malware of various sorts is propagated include the following: free and demonstration software, pornographic websites, games, e-mail, spam and discussion groups. Virus can also be present on material such as CD, diskette or USB key...

Many users have installed anti-virus software on their computers that can detect and eliminate known viruses. In reaction to this, criminals have created new kinds of viruses that try to trick the anti-virus software - two examples are **stealth viruses** and **polymorphic viruses**. A stealth virus hides itself from the anti-virus software by compressing the original file and creating an infected file of the same size. Stealth viruses can now be detected with modern anti-virus software that scans ordinary programs to find virus patterns. Polymorphic viruses modify their code after each infection, making their detection by signature quite difficult. One part of the virus is encrypted with a different key each time, leading to a different variant of the virus.

Today, the principle objective associated with viruses is no longer gratuitous large−scale data destruction. They are usually designed to make money. Their inherent characteristics facilitate their

use for fraud. Thus, viruses have become highly lucrative tools for organized criminals engaged in financial crime.

The following are generic common countermeasures to prevent virus infection and damages: (i) Resolve software security holes; (ii) Conduct virus scans regularly; (iii) update the virus signatures of anti-virus software; (iv) Do not open the attachment file to suspicious e-mail; (v) Check HTML source before updating web contents.

A **worm** is an independent program that is similar to a virus. A worm can also destroy files, but it does not need the help of a program to propagate itself through e-mail or Internet Chat Relay. Generally, worms compromise a network's capacity to perform by consuming bandwidth.

Example

A worm causes the slowdown of the Internet services of a specific country. Internet users complain heavily of a slowdown in logging services, e-mail services, downloading foreign website homepages, and other online transmissions. Major websites, such as those of online services and banks, are disrupted. Once emergency measures start, it takes several hours before the malicious code is under control. The total damages are difficult to estimate precisely, but the incident does have a serious impact on the economic life of the country.

A worm can corrupt documents frequently used by users, businesses and governments on all hard drives connected to an infected PC. It can even affect external data-storage devices. Worms are propagated through e-mails – often when attached to messages attracting recipients with subject lines such as "hot movie" for example. Once the recipient opens the attachment, a program disabling the anti-virus software can be launched. The malicious code may not necessarily aim to install *backdoor*[24] or keystroke loggers. Instead, it may aim to destroy all-important files on the computer. In order to accomplish this feat, the worm injects file-deletion instructions onto servers.

Worms can also infect mobile phones through Bluetooth for example. Once the worm is installed in the memory, it begins scanning for Bluetooth devices. This activity makes the phone unstable.

A **Trojan horse** presents itself as a useful or legitimate program, but it contains a malicious program that a computer automatically executes. Most often, malicious functions are spying functions, such as **packet sniffers**, **keyloggers**, or **backdoors**. These allow the attacker to gain remote access to the computer by bypassing normal authentication procedures. From there the hacker can spread malware, perform a DDoS attack, or erase data.

Example

An attacker sends e-mails that hide a Trojan horse. As soon as the Trojan horse is installed on the user's computer, the attacker gathers the user's confidential information, steals the user's identity, and subsequently removes money from the user's bank accounts.

The Trojan horse does not have the capability to spread by itself. Most often, Trojans are used to delude victims into running the program themselves. The effectiveness of a Trojan depends on the capacity to mislead the user while appearing to be a useful program.

Example

An attacker sends spoofed e-mails claiming to come from a well-known software company to lure victims by offering a new version of a specific software. In order to download it freely, the recipient has to click on an URL provided, which redirects the user to a phishing website to run a Trojan horse. Most often, malicious code are designed to steal banking or private information.

Using an attack "tool kit" available on the Internet, offensive codes can be implemented into popular websites, such as those of governments, hotels, and museums. These codes download a keylogger onto the computer of anyone accessing those sites, which allows the hacker to control the end-user system

[24] A **backdoor** or **trapdoor** usually refers to a portion of code incorporated into software that allows unauthorized entities to take control of systems, copy information, … without the owner's knowledge.

(information gathering, activities monitoring, etc.). Many users are vulnerable to this kind of attack without realising it. Identity and confidential information theft by Trojan attacks is becoming a real epidemic. Trojan horses are often the source that allows other forms of cybercrime. Tracking down the perpetrators of those crimes can be very difficult - prosecuting them, even more so.

Most viruses have a direct effect. Some have a delayed payload. Some wreak their damage while executing a specific action - this is called a **logic bomb**. Some wreak their damage on a specific date - this is called a *time bomb*. Logic bombs are viruses that are activated on a particular event, such as a birthday, to attack a system. None of these kinds of viruses should be confused with computer "bugs", which are programming errors, or more generally, design flaws that show up as functional problems.

A **keylogger (Keystroke logger)** is a program that monitors the keys typed by the user, and then either stores the information gathered on the computer or sends it directly back to a server. A keylogger is often installed on a computer through a Trojan horse, a virus or a worm. For example, one Trojan horse activates the keylogger as soon as some specific words like "credit card", "account", and "social security number" appear in a browser. The malicious program will then record everything typed by the user during a legitimate transaction and send the recorded information to the cybercriminal. Keyloggers are also widely distributed through *phishing e-mails* or *spyware* - and thereby often skirt anti-virus protection. Malicious websites intended to exploit web browser vulnerabilities are a widely used vector of propagation. *Keystroke loggers* are a very powerful cybertool. Worldwide keylogging attacks can be launched in few seconds on hundreds of computers, gathering confidential and personal data in order to commit large-scale financial crimes.

Many *malicious programs* are disguised as helpful *add-ons* for navigation, connection, or customization of services when in fact they are designed to perpetrate criminal activity. That criminal activity includes: (i) carrying out surveillance, such as information theft, password theft, and traffic surveillance: (ii) using computer resources; (iii) perpetrating attacks; and (iv) disseminating and controlling tools used for DDoS attacks. Thousands of these programs are in circulation. Their principal objective is financial gain.

Bots are programs (generally executable files) that are installed on a computer in order to automatically run a set of functions and to allow an illegitimate user to gain remote control through a communication channel. These infected computers, which run automated tasks for cybercriminals, are commonly named **Zombies**. The geographical location of the zombie machines stretches around the globe.

Bots never work alone. They are part of a big network of infected computers called a **botnet,** which stands for **bot network**. In every bot, a **backdoor** has been installed to be able to listen for commands. An Internet Relay Chat (IRC) channel or peer-to-peer network allows the cybercriminal to centrally control the zombies and to launch coordinated and simultaneous attacks.

Attackers mainly target computers that have broadband access to Internet and a low level of security. The main vectors of infection are the placement of an executable code downloaded: (i) by a Trojan horse; (ii) through e-mails; or (iii) via a malicious website. Bots also propagate by mass scanning to find vulnerabilities in services.

Cybercriminals control bots through communication channels. The most common control channel is the Internet Chat Relay (IRC): (i) because it is a popular protocol well adapted to run on different machines in a distributed way; and (ii) because it allows hackers to hide their illegal activities behind legitimate IRC traffic. Once a computer has been infected, it means that the hacker has established outbound connections to an IRC network, to a predetermined IRC server and with a specific channel to listen for commands from the master. Once the link is made, the cybercriminal has control of the bot - it is ready to receive commands and to launch attacks. The use of one central communication channel makes the bot system pretty vulnerable, since blocking specific TCP ports or taking down the IRC server immediately cuts the communication between bots and master. To get around this type of protection, attackers use communication methods like *peer-to-peer networks* or *VoIP*.

Some bots can use their own peer-to-peer networks to establish encrypted communication using random network ports. To evade detection and disjuncture, instead of using a central communication

channel, these bots maintain a list of compromised IP addresses. Therefore, the communication system is no longer centralized with only one checkpoint, and removing a peer from the network has no impact on the rest of the botnet.

Attackers use web-based controllers, such as the protocol HTTP, to control botnets and instant message controllers. VoIP can be a new and powerful communication channel for attackers and seems to be a better way for attackers to control their zombies, erase their tracks and cover up their attacks.

Botnet's owners either launch attacks themselves or rent their zombie computers network to anyone who wants to launch a large intrusion and attack. Bot-networks are thus a real threat to all Internet-connected systems and have a central role in the cybercriminal world. Various attacks can be performed by cybercriminals using bots and botnets. This includes:

- Drowning websites or servers (e-mail servers, …);
- Stealing identities by obtaining information from the victim;
- Proxying network traffic such as SMTP and HTTP;
- Phishing, by helping to identify potential victims and hosting fraudulent websites;
- Advanced fee fraud;
- Extortion, by threatening organizations with the launch of a DoS attack if they do not pay a certain amount of money;
- Hosting illegal data and installing malware such as a backdoor to maintain access after the exploit;
- Etc.

Any potential criminal can have at his disposal thousands of zombie computers ready to simultaneously launch an attack on one or several targets. In addition to being victims of attacks launched by botnets, organizations and users can run into serious problems with the law if it is proven that their computers have participated in a cyberattack.

Crimeware is another word to describe malicious software designed: (i) to perform illegal acts; (ii) to steal personal information; or (iii) to automate financial crime. Crimeware can include spyware, keystroke loggers and bots. Most often crimeware: (i) gathers confidential information, such as passwords or credit card numbers; or (ii) takes control of a computer and executes remote commands.

A **spyware** program watches users' activities, without their knowledge, gathers information such as online activities, confidential and personal information, and transmits this information back to the spyware's owner. Spyware represents a threat to privacy. It is used for identity theft, data corruption and personal profiling (Figure II.8). Usually, criminals use spyware to gather personal information, such as identity, passwords, and bank account numbers, to impersonate bank customers or to perpetrate illegal action in another name.

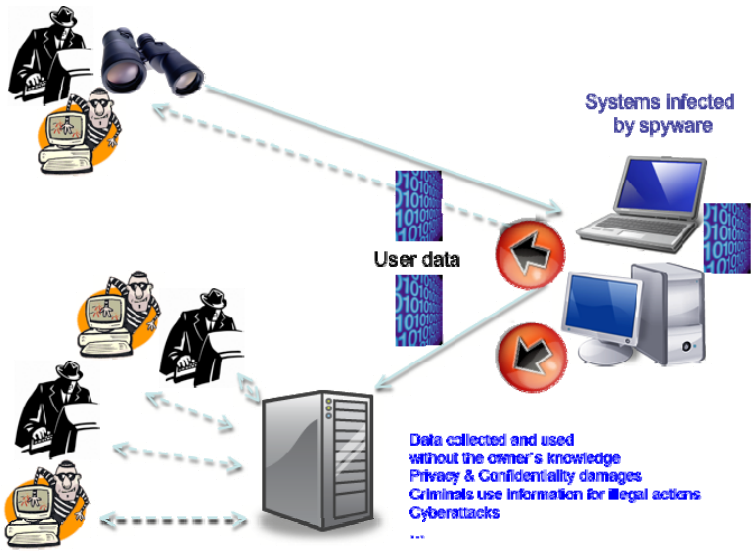

Figure II.8: Spyware attack

Another effect of a spyware attack is reduced computer system performance while spyware is working in the background and is connected to remote servers to upload the collected information. This creates the following concrete threats: (i) loss of network bandwidth; (ii) increased remote access costs; and (iii) frequent network crashes. Furthermore, firewalls cannot intercept spyware programs, because the program is downloaded at the will of the user, or through antivirus software that is not malicious by nature.

Example

In 2006, a plague of online identity theft hit online gamers of a particular country. The perpetrators created almost a quarter of a million fake famous "Lineage" game accounts using stolen identities. This mass identity theft contributed to an important black market run by gaming farms.

Criminals could steal thousands of names and ID numbers from online gamers via malware hidden in malicious websites. This is called **mass identity theft**. Generally, the player needs to enter his ID number to create an online account. Many websites require unnecessary personal registration, so they represent a big identity database from which *pharmers* can steal real login names, passwords and ID numbers. A pharmer is a person who perpetrates a *pharming attack* and redirects a website's traffic to another (bogus) website.

Statistics show that the average Internet user is a member of several websites, most of which request personal information. Usually, identification numbers reveal important information about their owners, such as gender, and place and date of birth. Therefore, a criminal can use stolen resident registration numbers to commit financial fraud and other damage.

Normally, spyware is bundled with another desirable program or downloaded in a peer-to-peer network. Spyware consists of two separate pieces of software: the **core functionality** and the **information-gathering functionality**. The core functionality is visible and attractive in order to draw the user into installing the program. The information-gathering functionality monitors the user's behavior and gathers information.

Spyware programs include an **End User License Agreement (EULA)**. Before downloading the software, the user has to accept the license and state the purpose for which the software will be used. However, users often do not read this information. Often they find that the EULA contains so much

information that either: (i) they do not know what to look out for; or (ii) they do not clearly comprehend the meaning.

The best ways to overcome these problems is: (i) to educate users about these threats; and (ii) to assign to an organization the task of defining policy rules regarding the downloading of software.

Far too often, users often do not realize the possible presence of a malicious program hidden in attractive software. The installation of **anti-spyware** programs is useful to block and remove spyware. This type of software combats spyware in two ways: (I) it prevents the installation of spyware using real-time protection by scanning incoming data and disk files at the time they are downloaded; and (ii) it tries to detect installed spyware and then remove it from the infected computer. A final precaution is to block unexpected requests for outgoing communications.

An attack may include a step involving the explicit or tacit approval of the user (in an adware attack, but never of a spyware attack). Whatever the means used to infiltrate, once it is installed, malware is turned to illicit use. Most commonly, a malware attack is executed without the consent of the user. Clandestinely, it collects and transmits data - for example, on websurfing habits, which are of interest for targeted advertising. It can act as a drone for illegal activities such as spam and phishing attacks, effectively working for the controller's financial gain. Detecting and uninstalling such software is not always straightforward. Frequently, users lack the skills and tools necessary to control these risks.

II.4.5 Cyber intrusion

Malevolent can attack a system by appropriating legitimate user identification and connection parameters such as passwords, or through deception and exploitation of vulnerabilities.

The main methods used to obtain the connection parameters of legitimate users to gain access to systems are:

- **Guessing**: The password is so obvious - such as the user's name, spouse or child, or a birthday - that the account is essentially unprotected. The user may also quite simply give out the password to the wrong person.
- **Deception** (**social engineering**): The attacker poses for example, as an administrator and asks for the password under some technical pretext. In a surprisingly large number of cases, users will reveal their data. The malevolent person can delude by telephone or electronic messaging. Some malevolent individuals are not computer geniuses, but simply crooks who maliciously obtain keys corresponding to the system locks they want to penetrate.
- **Listening to traffic**: The attacker intercepts or listens to unencrypted data transmitted over the network through communication protocols (*sniffing*, passive monitoring). Traffic analysis software for passive monitoring is generally delivered as a standard with various operating systems, while others are delivered as freeware on the network. They operate on any PC by "**sniffing**" and analyzing the data in transit on the lines, and then extracting passwords that are transmitted unencrypted by the user during connection. If fraudsters cannot rely on complicity from inside the organization in order to obtain passwords directly, they can electronically intercept from communication protocols or access files containing all the passwords.
- **Introducing a Trojan horse** or specific malicious spying program (spyware) onto the user's workstation to clandestinely record the parameters used to connect to remote systems. A Troyan is a small program that generally substitutes itself for the *login* code that requests the user's identification and password. The user supplies this information in the belief that he is in his normal operating environment. The password is immediately picked up and memorized by the Trojan horse, which then transmits it to the anonymous message server of the fraud. In the meantime, the real user would not have been able to connect since the real login program had not been executed. The user would probably have seen an "incorrect password error" type message and would think that an error had been made in keying in and would re-log, again giving identification and a password which would be treated by the real login program. One means of protection is to cipher the passwords so that if they are diverted, they are no longer

directly exploitable. The delinquent must then break the previously captured cipher passwords in order to use them.

- For an authentication system to function, all user passwords have to be stored on a server. Accessing the file that stores all the encrypted user passwords makes it possible to recover them. All that needs to be done is to **gain access and apply decryption software** - utilities are available, in particular on the network, for this purpose.
- **Cracking encrypted passwords**. If the malevolent person (or cracker) knows the cipher algorithm, he could test all the permutations that could possibly constitute the key for deciphering passwords. This is called a **brute force attack**. An alternative is to use a dictionary to find the encrypted password. This is called a **dictionary attack**. By successive comparisons of ciphered passwords contained in dictionaries, a criminal could guess the encrypted password used.
- **Spying on users** to record their connection parameters by using spyware or specific device, software or the user multimedia equipment (video camera and microphone that can be used to monitor the user's behaviour and spy on him), allows malevolent to capture confidential information, such as passwords to access protected systems.

Once in possession of the access key necessary to get into a system - the combination of user name and password - it is easy to penetrate the system and carry out all sorts of read and write operations. The challenge for the criminal is to avoid being detected and to leave no trace of his presence in the systems accessed. This may, in fact, be very simple for a capable of accessing a system that was supposed to be protected, he in all likelihood should has the capacity to delete or modify such potential traps as traceability audit files.

Whatever the mode of interception of the passwords, the users are unaware that their *logical keys* have been recorded by entities not entitled to do so in order to realize system intrusions. This is a threat for organizations as well as for individuals. They may be accused of perpetrating malicious incidents that were, in fact, carried out by someone else who usurped the user's account.

The following make it easier for malevolent to decrypt encrypted passwords rapidly: (i) the choice of obvious passwords; (ii) the power of PCs; and (iii) the common existence of password cracking software. The high number of passwords that can be decrypted in a second makes this activity open to virtually anyone.

On the *server side*, it is imperative to protect the access to the "passwords" file. No "anonymous" access should be permitted to this server The TFTP (**Trivial File Transfer Protocol**) facility, which allows access to files without authentication control, must be deactivated.

The following recommendations make password cracking more difficult:

- Use long passwords (at least 8 characters);
- Include a mixture of special characters (<,>,#,&, %, *,!, etc.), numbers, upper-case and lower-case letters;
- Change passwords regularly;
- Use a shadow password file, if this is made possible by the operating system.

In theory, users should take these considerations into account when they choose their passwords. In practice, this poses the painful problem of password memorization. Software exists that can be used to test a password's robustness.

The individual in charge of security must test the level of effectiveness of users' passwords on a regular basis. This can be done by using mechanisms identical to those that the malevolent person used to obtain and decipher the passwords.

A **sniffer** is a passive entity that listens to and records the data (as passwords for example) that crosses it without modifying the data. For this reason, its presence in a network is very difficult to detect. One

method of restricting the sphere of activities of a sniffer, is to strongly segment the network by bridges, routers or switches. This makes it so that the sniffer is effectively active only on one segment of the network. This type of security measure, which relates to the network architecture, is called "**proactive**".

Usually, network and system administrators use these peripherals and techniques of monitoring to monitor network activities. The same tool or technology can be utilized in different contexts, and with contrasting purposes: to improve the quality of network services, or to attack systems.

The only method that offers a reasonable protection from password theft is the one based on **single-usage passwords (one-time passwords)**. These are widely used for financial transactions.

A method can be implemented through **smart cards** and ad hoc devices that generate unique passwords. This dispenses with the need for the user to memorize and enter passwords that are too long or complex. However, all systems have a weak spot, and this type of authentication is no exception. This authentication procedure is based on synchronization between the user's device and the remote authentication server. A hacker could capture a password and reuse it immediately following the de-synchronization of the systems, which the hacker has provoked by modifying the system clocks.

Identification can also be carried out using a physical characteristic of the person, such as a fingerprint. This is called **biometrics**. It is not yet widespread enough for access control mechanisms. The physical characteristics of individuals must be captured and converted into a reference sample for storage in a database in order to, identify them and validate their identification, As it is digitized, the data becomes fragile - and hence modifiable - and must therefore be provided with the best possible protection. For each access request, the user's biometric data must be captured. This raises the possibility that the user will object to the capture method. The feeling of intrusion makes this method unwelcome to users.

II.4.6 Spam and phishing

Spam is the bulk sending of unsolicited e-mail: (i) for commercial or publicity purposes; or (ii) for purposes of introducing malicious software, such as malware and crimeware, into the system. At its worst, spam resembles an e−mail bombing attack, with overloaded mail servers, full user mailboxes, and the attendant inconveniences.

Previously, spam was regarded primarily as a *nuisance*, but nowadays spam e-mail represents a **real threat**. It has become the privileged vector for the propagation of viruses, worms, Trojans, spyware and phishing attempts. The coordination of spam and **botnets** (*robot networks*) is an ideal tool to commit *DoS attacks* by flooding servers with thousands of e-mails.

Spam not only decreases user productivity; it also increases storage and bandwidth costs for organizations.

The term **phishing** refers to an attack using mail programs to trick or coax web users into revealing sensitive information that can then be exploited for criminal purposes, such as fraud or embezzlement (Figure II.9).

In general, criminals conduct phishing attacks by using e-mail messages that are forged to appear as though they come from a genuine institution with which the user may have dealings (e.g. the post office, a bank, a dealer, or an online auction site). Attackers may also use a telephone call, instant messaging (IM) or cell phone text messages. They may even approach victims in person.

Examples

Customers of a bank receive a spoofed e-mail explaining that the bank is doing upgrades and that they have to confirm their account details. Customers are then asked to click on a link that directs them to a forged website. Several variations of this scheme exist based on a scammed e-mail luring a bank's customers to a spoofed website.

A hacker sets up a phishing site imitating the website of a particular bank. He sends e-mails to bank customers warning them of the closing of their bank account if they did not update personal information. He lures his victims to a fake website, and induces them into entering their account number and password. The hacker makes sure that he sends the scam e-mail from an address that looks as legitimate as possible – he designs the website link, and the fake website itself so that they look as authentic as possible.

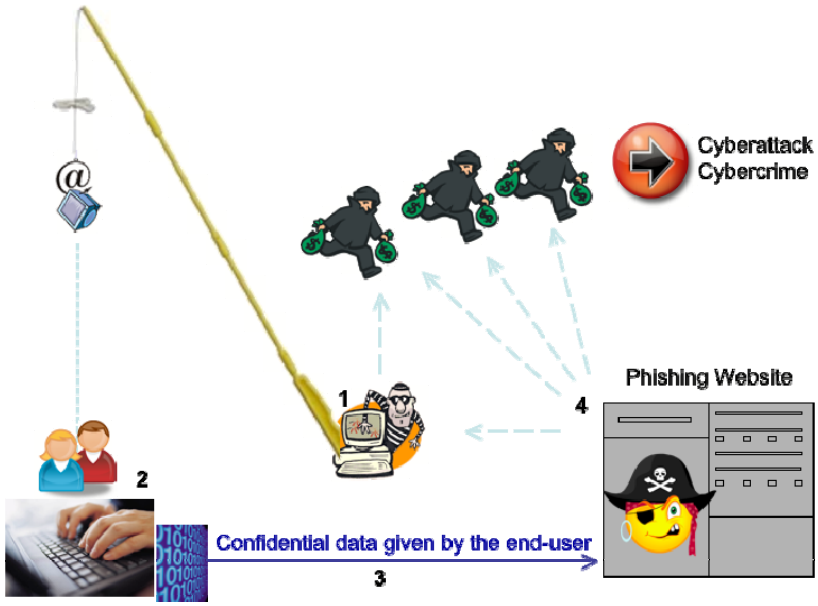

Figure II.9: Phishing attack

Phishing attacks rely on social engineering and technical practices. They aim to gather confidential information by luring the user with a message that is supposed to come from a legitimate organization. Most often, the motivation is financial gain. Phishers either commit fraudulent acts with the information they collect, or they sell that information online.

Spam is the main tool used to reach a maximum number of potential phishing victims. The phisher can use spammers' databases that contain a large number of e-mail addresses in order to send them e−mails that look as much as possible like legitimate requests - e-mails bearing the logo and colors of a company with which the user is very familiar. Phishers use botnets in order to simultaneously launch a large number of phishing attacks. The most common lure is an e-mail asking the user to update his account or change his password for security reasons. Cybercriminals know that organizations are now aware of these attacks and have taken preventive security measures against them. Those criminals keep making their own adjustments – they keep inventing new methods to circumvent detection tools.

Example

A hacker targets a phishing attack at taxpayers. He sends users a fake e-mail that claims to come from the national tax authority. The scam e-mail claims that the recipient has either submitted an incomplete tax declaration or has not completed one at all. Users are requested to click on the link provided in order to correct the mistake. The fake website hides a malicious code, and as soon as the user opens the website, a Trojan horse and keylogger is downloaded on the customer's computer.

The use of instant messaging as a propagation vector of malware and lures is on the rise. Phishing attacks are particularly *insidious*, because the lure messages sent by the phishers appear to the user to come from someone on the contact list. A victim is less likely to suspect an instant message from a

friend than an e-mail from some organization. Generally, phishers try to reach as many potential victims as possible, but a new trend exists: **spear phishing**. These attacks are more targeted than lure phishing: the attacker has to collect or steal inside information to increase the feeling of legitimacy. This has given rise to a growing new trend called **vishing**. This is a phishing attack that involves *Voice over IP* (VoIP) – hence, "vishing". The criminal sends an e-mail that contains a telephone number reachable by VoIP technology. The message claims to come from a legitimate source and requires the recipient to call the number. In other words, it unfolds just like any other phishing attack, except that the victim is asked to make contact via a VoIP number instead of by clicking on a link. The victim calls the number, and the attacker asks the victim to give out personal information directly over the phone.

Phishing attacks can be divided into the following categories:

- **Deceptive attacks** that rely on fraudulent messages;
- Malware attacks;
- **DNS-based attacks** that rely on the alteration of the lookup of host names to redirect the user to a fraudulent server;
- Content-injection attacks.

Deceptive phishing is the most common phishing attack. A deceptive phisher impersonates the sender by spoofing the source e-mail using known flaws in SMTP, the common mail server protocol. The deceptive e-mail will always ask the user to click on some link in order to fix a problem quickly and safely. To increase the probability that a user will believe the message is genuine; attackers may use various techniques. These include: (i) employing IP addresses (numerical addresses) instead of domain names in hyperlinks for the fake website; (ii) using cousin domains by registering similar DNS domains with minor URL changes; and (iii) using HTML-based e-mail in order to mask the website's URL.

Malware-based phishing is on the rise. These attacks rely on social engineering practices: They lure the user into opening an e-mail attachment or downloading some interesting software that contains malware. These attacks also rely on technical vulnerabilities that allow the malware to propagate itself by taking advantage of security vulnerabilities.

DNS-based phishing is another increasingly popular method. These attacks draw the user to a malicious website embedding malicious content. This malware is mostly comprised of: (i) Trojans or keyloggers that gather credentials by recording keystrokes; (ii) screenloggers that monitor screenshots from the computer; and (iii) redirectors. Once installed on the computer, redirectors are useful tools for luring victims to an unwanted location. The malware is used to install a malicious **Browser Helper Object**. The latter is designed to control the Internet Explorer web browser and redirects HTTP traffic to illegitimate sites. Malware can also be used: (i) to manipulate the host files that are used to maintain a mapping between DNS addresses and IP addresses; and (ii) to manipulate other DNS-specific information on the targeted PC. As soon as the malware has inserted a fake DNS entry, the user will not notice that the web browser is connecting to a phoney website instead of the legitimate one.

A more advanced DNS-based attack is called **pharming**. This relies on a DNS spoofing method that compromises the integrity of the lookup process for domain names. These attacks poison the DNS cache, so that it will redirect users to a phishing website. It accomplishes this by inserting false IP addresses for key domain names. Pharming does not rely on a social engineering impact to lure victims to fake websites. **DNS spoofing** represents a real threat to misconfigured legitimate or privately controlled DNS servers.

Content-injection phishing makes use of code insertion into a legitimate site. Once the hacker has inserted the code, he can either use the malicious content to redirect the victim to unexpected websites, or install malware on the victim's computer. Hackers often inject malicious content into a site through **cross-site scripting vulnerability**, which is the result of poor development processes. The malicious content then becomes part of the data stored on the legitimate site.

Because of all the options they provide to criminals, phishing attacks have become one of the most significant online security threats. They aim: (i) to steal confidential information for financial crimes or identity theft; and (ii) to install malware and extend zombie networks causing substantial financial losses and personal damage.

II.4.7 Some communication protocols misuse

A **TCP spoofing** attack relies upon the fact that the TCP protocol establishes a logical connection between two end-systems in order to support data exchange.

Logical identifiers (port numbers) are used to establish a TCP connection. Some port numbers are fixed and well-known - reserved for particular programs. Others are allocated dynamically during the connection, according to a specific algorithm. A **TCP port number attack** involves guessing or predicting the next port numbers that will be allocated for data exchange in order to use those numbers instead of the legitimate user - effectively hijacking them. This makes it possible to pass through firewalls and establish a "secure" connection between two entities - the hacker and the target. Meanwhile, the legitimate remote user's access to the facility is of course blocked, but it is simple enough for the hacker to send a message saying that the requested system is inactive.

In order to prevent this sort of incident, the firewall must be configured correctly, so as to disallow the passage of IP packets possessing an internal IP address arriving at external communication ports. The firewall's authentication procedure should not be based solely on an IP address - it should utilize additional encryption functions.

User datagram protocol (UDP) is a connectionless transport protocol. It is an alternative to TCP for the rapid transfer of a small volume of data. UDP communications are not subject to any control mechanisms, so there are no checks for identification, flow or error. As a result, anyone can use the IP address of an authorized system user in order to penetrate it. An attacker can perpetrate a UDP session theft without the application servers even being aware of it (**UDP attack**).

Knowledge of Internet protocol operational modes and weaknesses can make it easy for criminals: (i) to mystify systems in order to modify packet routing and delivery by usurping IP addresses (IP spoofing); or (ii) to lure systems and get control of them.

Attackers can easily redirect packets towards a destination of their choice by using certain optional IP features that serve to define the route. They can specify the addresses of the intermediary systems through which the packet must pass, and then falsify those addresses.

Attacks at routing level are based on hoaxing routers, gateways and destination stations by providing false addressing information that enables the data to be re-routed. A criminal can easily set up the routing mechanics so that packets will be redirected to illegitimate destinations. He does this by exploiting optional features of Internet protocol that enable the route to be defined: Those optional features are called **strict source routing** and **loose source routing**. In other words, the criminal rigs the system by falsifying the addresses of the intermediate systems through which a packet passes (**source route falsification attack**).

An attack perpetrated by preying on the **Routing Information Protocol (RIP)** is an example of router mystification. In the context of normal usage, RIP protocol contributes globally to a correct routing process. A hacker can corrupt it so that it will re-route communications and prevent them from reaching their intended destinations. All that is required is to send false routing information to the gateways and the target station, by simulating an authorized sender. The victim uses the IP address provided by the hacker in the RIP packet to transmit data to the destination of the supposed emitter, who is in fact none other than the hacker himself (**RIP protocol attack**).

Internet data packets contain user data as well as the source and destination IP addresses. Routers use these addresses to execute their routing function. Internet protocol exclusively contributes to elementary functions relating to the routing of data, and in no way checks the manner in which the routing is performed and executed. Consequently, there is a need for a routing control protocol. **ICMP (Internet Control Message Protocol)** was developed to fill this role. Its purpose is to create control

messages that are transferred by the Internet protocol. Thus, if a router detects a routing problem, it informs the emitter by sending an ICMP message.

Once a hacker knows the operating mode of this public protocol, it is easy to perpetrate an **ICMP attack** by generating false ICMP messages. A massive number of such messages can *overload* the network. **Flooding the network** with false ICMP messages can render it unusable. Consequently, there is a need for security relating to the availability of the network and service denial. Hackers know very well how to use ICMP to do the following:

- Paralyse the network by redirecting IP packets to a false destination, such as their own address;
- Substantially increase the load on systems by making them pointlessly process a large number of ICMP messages;
- Stop an emitter from sending data by exploiting the packet emission flow control feature provided by ICMP. This also has consequences for the traffic supported by the network and damages its performance (reliability, operational dependency).

Nothing can really be done to prevent this kind of attack, apart from configuring routers so as to stop them from generating more than a certain number of ICMP messages during a given time period. The supervision function in network administration systems can be used to detect an unreasonable number of ICMP messages and to generate an alarm when an abnormal number is detected.

Attackers know how to exploit not only operational features of communications protocols, but also the characteristics of the various operating systems and the ways in which they work. Thus, by overloading certain buffers (**buffer overflow attack**), it is possible to provoke a serious malfunction or system crash. The targets of this type of attack are, of course, those systems that provide an important service, either for data transfer or for name and address management. Most attacks on websites exploit flaws in the operating system in order to shut them down, thereby making them unreachable.

A buffer overflow attack damages computers and applications by exploiting their internal operational characteristics - in particular, those of the operating system. One way is for the hacker to subject those internal operational characteristics to a capacity exceeding certain buffer zones[25]. This leads to serious dysfunction - it can cause a system to crash. As discussed earlier, the law considers the type of attack that causes a denial of service to be a criminal act. The following are ways to decrease the risk of dysfunction: (i) using secure operating systems; using non-permissive configuration; and (iii) having an effective management plan.

II.4.8 Cyberattack methodology

The process of committing a cyberattack consists of collecting and searching for the vulnerabilities of the target systems and exploiting them.

[25] A buffer is a limited space of storage memory.

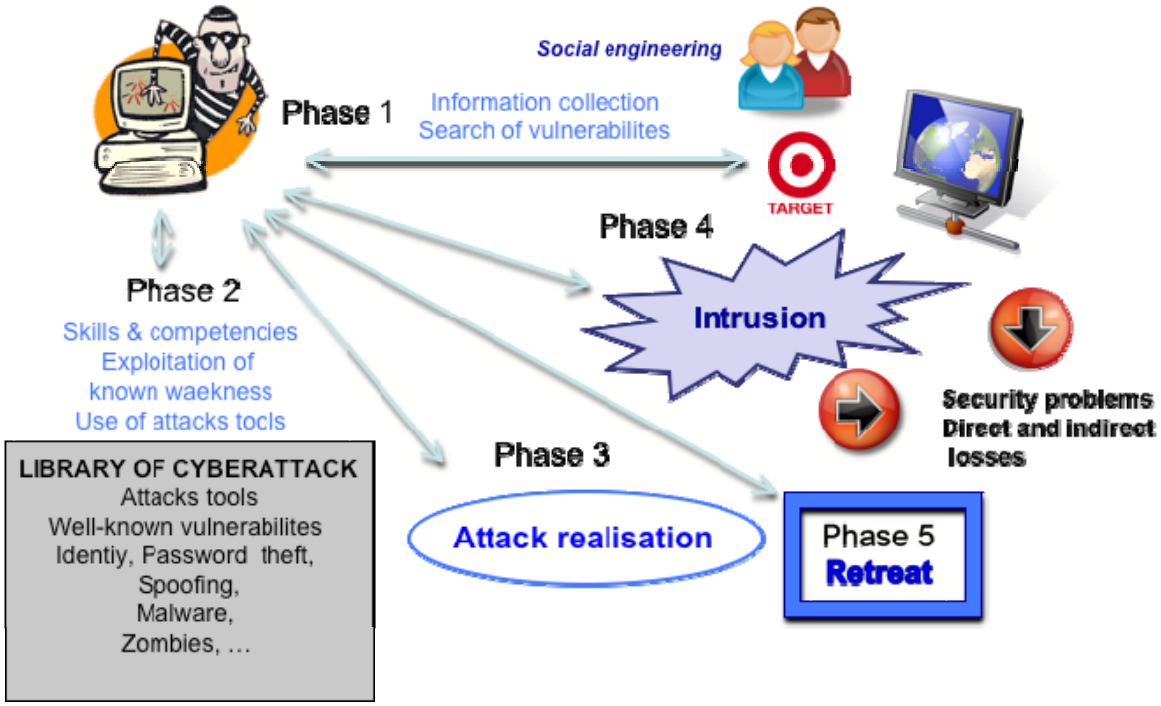

Figure II.10: Cyberattack methodology

Figure II.10 illustrates the different phases of a cyberattack. During the first phase, the attacker gathers information and searches for potential vulnerabilities within the target system, in order to gain a maximum of information for future exploitation. He studies the mechanisms and levels of security used for identification, authentication, access control, encryption and surveillance. He identifies technical, organizational and human weaknesses of the targeted environment. Frequently, the attacker will attempt to coax naïve or credulous users into revealing information that he can use to design an attack. This is called social engineering.

Criminals also look for and exploit security vulnerabilities that have been identified, but have not yet been repaired (patched). They use whatever means are available – such as attack libraries or attack toolkits – to infiltrate the system. During the retreat phase, the attacker tries to cover up the traces of the attack, or to ensure that whatever traces are left cannot be linked to him. Criminals increase their anonymity by using aliases, usurping legitimate users' identities, or covering their tracks by means of multiple intermediate (relay) systems.

The conditions for a successful attack are:

- **Knowledge** of the target system, including its function, service, configuration, security policy and tools, and administration;
- **Efficient use** of programs that automatically exploit vulnerabilities for breaking into a computer – these programs are called "exploits";
- **Capacity of the aggressor to cover his tracks**, in order to avoid being detected and identified;
- **Rapidity of the attack** – the faster the attack, the more likely that the security measures will take effect too late.

If the attacker does not know the target well (phase 1 of the attack is inadequate), the risk of being tracked down increases.

The following types of systems are vulnerable to an attack (Figure II.11):

- A security system, such as a firewall or an authentication server;
- A security-related system, such as a router or DNS;
- A system that has no link to security measures, services or functions, such as a workstation or a web server.

The type of system targeted determines: (i) the degree of difficulty involved in carrying out the attack; (ii) the speed with which the attack can be detected; and (iii) the level of destruction caused by the attack.

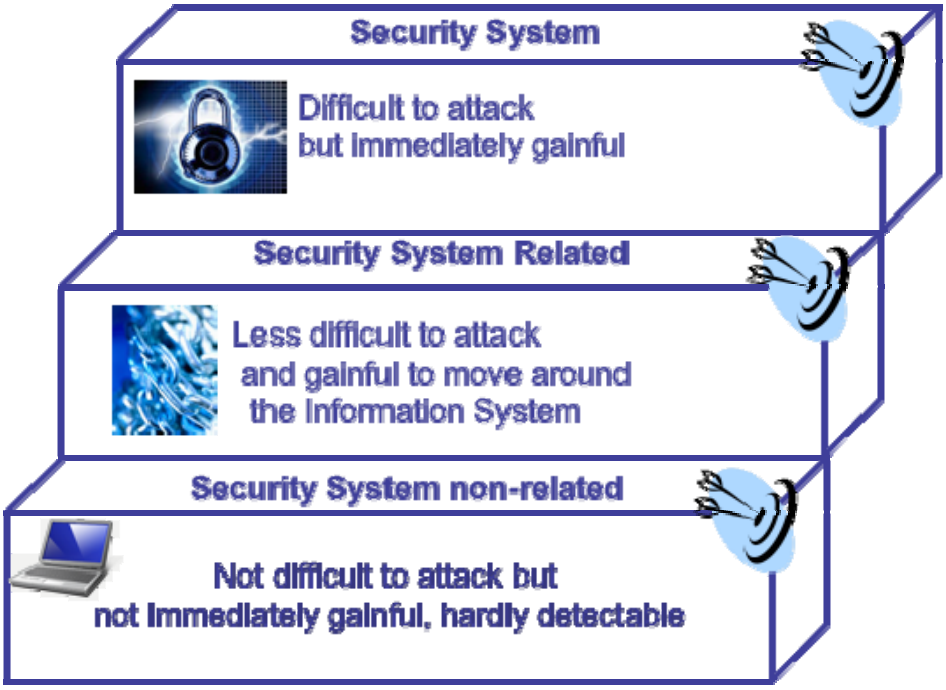

Figure II.11: Targets of cyberattacks

In any case, the computer attacker exploits the *weaknesses of the target system*. Because computer systems are complex by nature, they are always vulnerable. Even *security systems are both vulnerable and fallible*. Some systems are easy to attack; others are much less so. There is no method of security that can guarantee full protection.

In order for an organization to react effectively to an attack, it needs to identify the visible objective of the attack and the means used to carry it out. The following questions must be adequately answered in order to improve incident management and adapt reactions: (i) What phase is the attack process currently in? (ii) What damage has been caused by the attack? (iii) Who is the attacker?

An organization needs to make in depth documentations of any incidents in order to effectively adapt its security policy to the new “post-crisis” context. It also needs to monitor its information system daily, particularly its network, in order to identify attacks as rapidly as possible so that those attacks can be countered efficiently.

II.5 COMPUTER-RELATED CRIME AND CYBERCRIME

II.5.1 Definitions

The vulnerabilities of digital technologies and inadequate control of them combine to create an environment of *insecurity*. Criminals naturally take advantage of this state of affairs. Criminals can potentially exploit every technology for illegal purposes; the Internet is no exception, as the criminal presence in cyberspace amply demonstrates.

In 1983, OECD[26] defined **computer−related crime** as any illegal, unethical or unauthorized behaviour involving the transmission or automatic processing of data.

A computer-related crime is one in which the computer system is either the object of the crime; the means of committing the crime; or both. It is a crime connected to digital technology - a subset of white-collar crime. **Cybercrime** is a form of computer-related crime committed using Internet technology - it covers all crimes committed in cyberspace.

In the virtual world, crime can be automated. This means that a hacker could launch a large-scale cyber-epidemic remotely via a network, with the possibility of delayed action. This frees the criminal from the usual constraints of time and space (Figure II.12).

Internet technology facilitates a wide range of infractions. These include for examples:

- Theft;
- Information sabotage;
- Copyright infractions;
- Breach of professional trust;
- Digital privacy;
- Intellectual property;
- Distribution of illegal content;
- Anti-competitive attacks;
- Industrial espionage;
- Trademark infringements;
- Disinformation;
- Denial of service;
- Various forms of fraud;
- Etc.

Cybercrime is the natural extension of ordinary criminal activities. Today, criminal acts are committed across cyberspace, using non-conventional means in a manner that is complementary to ordinary crime.

A computer-related crime can be expressed through different expressions. These include:

- White collar crime - most often this term is associated with financial or economic crime, and could involves organized crime;
- Technological, high-technology, or high-tech crime;
- Computer and internet-related crime;

[26] OCDE: Organisation for economic co-operation and development - For a better world economy - http://www.oecd.org/home/

- Computer assisted crime - as in fraud or money laundering:
- Computer focused crime - as in website defacement;
- Digital crime;
- Electronic crime;
- Cybercrime.

Whatever it is called, a computer-related crime is complex. It can be committed: (i) by force, such as breaking into a computer system or telecommunication line; or (ii) by fraud or deception, such as scams and cons.

The Internet not only provides ideal conditions for new illegal projects and activities, but also opens up the opportunity for new variations on old crimes, such as fraud. The Internet makes it easy to find and exploit new means of making money. Naturally, this empowering feature is not lost on the criminal world. By embracing information technologies, criminals hope to increase their profits while minimizing their exposure to risk.

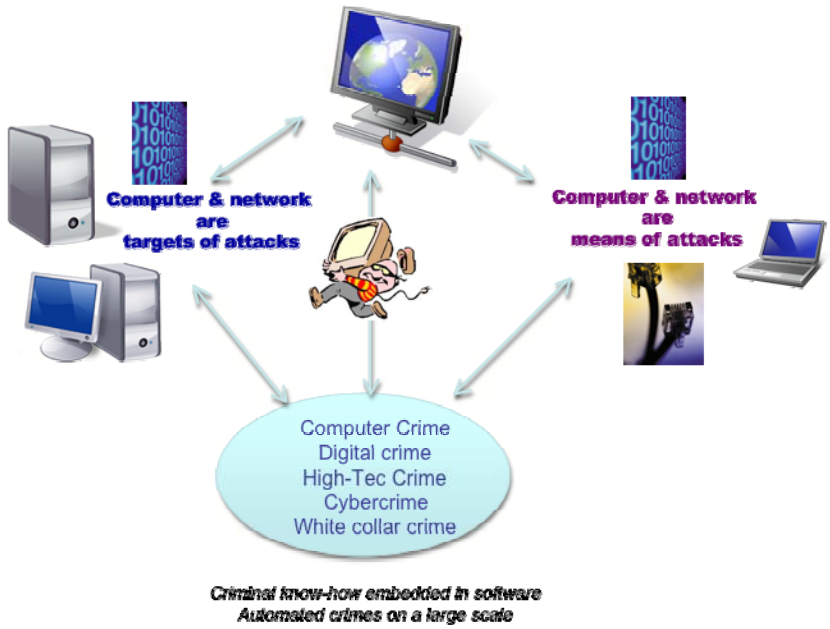

Figure II.12: The nature of computer – related crime

The Organized crime situation report 2005 by the Council of Europe[27] divides cybercrime into the following types of offences:

- **Offences against confidentiality, integrity and availability of information and communication infrastructures:** illegal access to computers by computer hacking or wiretapping, or by deceiving internet users by spoofing, phishing or password phishing, computer espionage, computer sabotage and extortion;

[27] www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/8_Organised_crime/Documents/Report2005E.pdf

- **Computer related traditional crimes:** frauds, manipulations, abuse of credit cards, forgery, online grooming of children, search for victims, attacks on public safety through manipulation of flight control systems or hospital computers;
- **Content-related offences:** child pornography, racism, xenophobia, soliciting, inciting, providing instructions for and offering to commit crimes ranging from murder to rape, torture, sabotage and terrorism, cyberstalking, libel and dissemination of false information, Internet gambling;
- **Offences related to infringement of copyright and related rights:** unauthorized production and use of software, data, audio, and video.

These categories of offences correspond to the categories defined in the Convention on Cybercrime (ETS 185) and the Additional Protocol to the Convention on Cybercrime(ETS 189)[28] . related to criminal acts of a racist and xenophobic nature committed through computer systems

II.6 THE PRINCIPAL FORMS OF INTERNET RELATED CRIME[29]

II.6.1 Swindles, Espionage and Intelligence Activities, Rackets and Blackmail

The *various common forms of organized crime* - protection rackets, human trafficking, confidence schemes, theft, etc. - can benefit from using the Internet. By making it easy to communicate, the Internet assists those engaged in any form of *smuggling* - whether it be of arms or human beings - and *swindles* - whether it be attacks against property, computer systems or infrastructure, data theft, copyright infringements, etc.

Some cybercriminals use another person's identity in order to make purchases on the victim's account. They frequently carry this out by means of credit-card fraud. For example, a criminal might create valid card numbers that do not correspond to any real account. He would use the information to purchase something online, and use a "disposable" address for a one time delivery. The cost would be borne by the bank system or the merchant. A specialized gang may victimize card users after obtaining their credit-card numbers from a pickpocket or a dishonest merchant.

Another category of swindle involves *the sale of imaginary services*, such as diplomas from non-existent universities, diplomatic passports from non existent countries, and auctions of non existent products.

The web also facilitates **espionage** and intelligence work by making it easy to illegally intercept information being transferred over the Internet. Ironically, the systematic use of secure means of communication by **professional terrorists** can help them to operate with greater impunity, by reducing the amount of information that is vulnerable to interception by law-enforcement authorities.

The Internet is a powerful medium that lends itself to the dissemination of methods of committing crimes and illegal acts, encouraging potential criminals.

II.6.2 Information Manipulation

Manipulation can take many forms, such as leaking internal documents in order to *destabilize* a company, or sending e-mail requests for charity donations via false sites.

It is easy for nefarious individuals to *spread rumour* and *disinformation* via the Internet. This can take the form of infractions against the media law, criminal incitement, apology of crimes against humanity, apology of and incitement to terrorism, incitement to racial hatred, historical revisionism (negationism), character assassination, insults, etc.

---

[28] www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
and www.conventions.coe.int/Treaty/en/Treaties/Html/189.htm

[29] This section is adapted from S. Ghernaouti-Hélie's publication "Information Security for Economic and social development" - ESCAP, UNITED NATIONS - Bangkok, 2008 - http://www.unescap.org/icstd/policy/

II.6.3 Economic Crime and Money Laundering

Economic crime via the Internet is not limited to organized crime. Modern ICTs allow isolated individuals to engage in economic crime, either alone or in concert with groups of various sizes.

Criminals can organize themselves around the exchange of information, thanks to the use of ICT. Networks can bring together individuals and expertise to organize a virtual criminal gang.

Given the high degree of economic expertise and skills that economic crime requires, it is an obvious candidate for "improvement" by means of Internet. The Internet contributes to the acquisition of information and the knowledge of markets, laws, technology, etc. that are needed to commit economic crimes. It can also be used to prospect for victims. Economic crime is influenced by new technologies, which become part of the criminals' repertoire and place information at the heart of their strategies and decision-making processes. New technologies can facilitate theft of all kinds, including tampering, information sabotage, fraud, blackmail, extortion, protection rackets, and ransom demands.

In effect, information resources become potential hostages of the cybercriminals. *Blackmailers* have extended their operations to cyberspace, and anyone who takes part in cyberspace may suddenly find himself or herself the victim of attempted blackmail, disinformation or propaganda. Furthermore, there has been an explosion in identity theft since 2003, due to the opportunities presented by cyberspace. This demonstrates that criminals have not been slow to recognize the benefits of anonymity that the Internet affords, or the ease with which they can use false identities to avoid prosecution or criminal and terrorist responsibility. Identity theft, readily performed via the Internet, is a major factor in illicit activities.

Money-launderers increasingly use the Internet to launder money that is generated by traditional criminal activities such as drug trafficking, arms smuggling, corruption, prostitution, child abuse, and tax fraud.

Although it is greatly under-reported and frequently invisible, money laundering via the Internet is increasingly popular. The Internet is an ideal vehicle, thanks to its virtual nature (anonymity, cyberspace, speed of transfer) and its freedom of territorial constraints (cross-border nature, conflicting competence and jurisdictions). The Internet makes it possible to channel monies of criminal origin into legitimate economic circuits using money transfers, investment and capitalization.

The following services make it possible for criminals to generate seemingly legitimate revenues that are difficult to monitor and almost impossible to prosecute: (i) online investment; (ii) online gambling; and (iii) online commerce, which can be used to “sell" imaginary goods and services for real money. The following can all be used to launder the proceeds of crime: (i) e-banking; (ii) real estate transactions via the net; (iii) virtual front companies; and (iv) electronic cash. Ordinary users may unknowingly enable money laundering when they use certain virtual services. Commercial organizations may also unwittingly become involved, with all of the potentially disastrous legal and commercial implications that entails. This is a *major source of risk* for companies.

Currently there are few effective means of controlling the phenomenon of Internet-enabled money laundering.

The ease with which digital information can be reproduced has spawned a market for illegal copies and **piracy**. It accounts for many tens of billions of US dollars in losses for publishers of software, music and video films. There has also been a great increase in the number of scholarly and academic works resorting to plagiarism simply by copying existing documents from the web. There are a great variety of possible intellectual property infractions: forgery of an author's work (including software), design, model, trademark, etc.

II.6.4 Threats against States and cyber terrorism

National security, public safety, and effective functioning of an economy rely on infrastructures that are essential for states, organizations and individuals. The nature of critical infrastructures and the degree of importance vary from country to country.

The following sectors can be considered as **critical infrastructures**: (i) communication; (ii) energy, water, and transportation: (iii) financial; (iv) medical services; and (v) government services.

The vulnerability of the essential infrastructures of a country is increased as the use of ICTs takes root. Critical infrastructures are currently controlled or accessed via information and communication infrastructures that mostly belong to private or foreign actors and are administrated by the private sector. Some examples are producers and distributors of electricity, and telecom operators.

Cybercrime can take on a terrorist dimension when the systems targeted are part of a critical infrastructure.

Adversaries to states or organizations can attack systems or infrastructures in order to profit from them, destroy them, or find material for blackmail. Vulnerabilities of ICTs can be exploited in pursuit of political goals.

According to the Center for Security Studies in Zurich: "Threats or risks in the field of critical infrastructures are variable concerning the type of infrastructure considered. Reducing the risks to critical infrastructures requires an effort to counter or disrupt the sources of threats through education, civil action, criminal prosecution, or intelligence education" [30].

Particular emphasis needs to be placed on the electrical power generation and distribution systems, which are essential to the operation of most infrastructures. One of the key objectives of *cyberterrorists* appears to be the control of critical infrastructure elements. This is demonstrated by the increase in the number of scans (probing for vulnerabilities that can be used to penetrate the system at a future date) targeting the computers of infrastructure operators.

At the present time, there is *no universal definition* of what constitutes **cyberterrorism**. The simplest way to look at it would be terrorism applied to cyberspace. Terrorism is generally understood to mean the systematic use of violence to achieve political aims. By extension, cyberterrorism could be defined as the systematic use of violence in cyberspace to achieve political aims. Or better yet, the systematic attempt to cause *debilitating destruction (or debilitating disfunction)* in cyberspace, in order to achieve political aims. One key question is whether cyberterrorism will be defined to refer exclusively to terrorism carried out at least in part through virtual means, or will it include the physical destruction – such as by a bombing – of physical infrastructure that underpins cyberspace. If it is the latter, then cyberterrorism might be defined as *the systematic use of any kind of violence* that is intended to debilitate the cyberworld, in order *to achieve political aims*.

It is entirely legitimate to ask whether the breakdown of the Internet, or a portion of it, as a result of malicious acts, might not sow terror within the community of web users, some groups of economic players, and the general public. Contrarily, we may be dealing in the main with instances of economic terrorism, aimed at damaging organizations that use the Internet for their activities.

The term cyberterrorism, which has come into vogue since the September 11 attacks, should be used with discretion. It should not be forgotten that the very first widely publicized Denial of Service (DOS) attacks, on February 10, 2000, were the work of a fifteen-year-old who went by the nickname of "Mafia Boy". The youth was identified and apprehended several months later. Although the reasons for his actions remain unknown, it is highly unlikely that they were political in nature. If the same attack had been carried out after the events of September 11, it might have immediately been classified as cyberterrorism. In the absence of something concrete, such as a claim of having perpetrated the attack, or a piece of physical evidence that can be linked to a terrorist organization, it is difficult to attribute an attack to cyberterrorism.

The term cyberterrorism covers a fairly vague catalogue of *new threats*, and it is difficult to speculate what the motivation or aims of an unknown attacker or group of attackers might be. When the only thing known is the target of the attack, it is very dubious to conjecture on what may have been the motivation behind a cyberattack. Was it sport, terrorism, mercenary, activism, material gain, personal or group vendetta? Without something concrete to go on, who knows?

---

[30] International Critical Information Infrastructure Protection, vol.II, p.63 – Center for Security Studies, ETH Zurich.

Nowadays, terrorists use ICTs to perform hostile actions for political objectives. They use the Internet as a means of recruiting new adherents - websites can contain photos, interviews and training videos). Terrorists use ICTs to incite, recruit, train, finance, and gather information, all for the purpose of subsequently carrying out attacks outside of cyberspace.

Cyberterrorism constitutes an extremely menacing new threat, whether it takes the form of destabilizing economies, threatening critical infrastructures, spreading ideology, or manipulating information. Apart from its threat to information systems and the cyberworld in general, it can endanger human life by creating an indirect menace to life and limb.

II.6.5 Crimes against persons

Cybercrimes against persons can be divided into the following categories: (i) pornography; (ii) libel; (iii) dissemination of offensive material; (iv) cyberstalking; and (v) incitement to commit crime.

The Internet makes it possible for clandestine virtual communities to form around practices that are subject to legal sanction. This may involve pornography, pedophilia, or so-called snuff movies - films showing scenes of violence and torture on real life victims that can sometimes result in their death. This type of crime is commonly linked to human trafficking, which most often involves women and children. The Internet allows perpetrators to share films and photos with greatly reduced risk of police detection. The servers are frequently located in countries where law enforcement is absent or ineffectual. Criminals can operate more freely due to the following Internet options: (i) private internet relay chat (IRC) services that can be used for very limited periods of time; and (ii) peer-to-peer (P2P) exchanges.

The Internet is a means through which cybercriminals can produce and distribute child pornography. Pedophiles may use the Internet to contact children in order to lure them into situations where those children become victims of sexual abuse. Crimes specifically against minors include the dissemination of pornographic messages that may be seen by minors.

There are a wide variety of national laws from one country to another that ban sexual abuse and child sexual abuse. The age of sexual consent varies from country to country. Child abuse criminals can profit from this fact by storing child pornography on servers in countries that are especially lax in this area of the law.

Other examples of crimes against persons include: (i) violation of privacy; (ii) defamation of character; (iii) betrayal of professional confidentiality; and (iv) hate speech.

Cyberstalking is the use of the Internet for stalking purposes resulting in online harassment or abuse. The following behaviours in cyberspace are linked to cyberstalking or cyberbullying: (i) transmitting threatening messages; (ii) spying on an individual’s activities; (iii) violating an individual’s privacy; and (iv) subjecting an individual to fear or emotional distress. These behaviors may be carried out by means of unsolicited e-mails, viruses, or unwanted electronic communications. They may take the form of defamatory or derogatory statements or negative rumors on web pages, forums, bulletin boards, or chat rooms.

Cyberbullying is the use of strength or power through e-mail, instant messaging, text messages, websites, or blogs to intimidate, annoy, frighten, or hurt an individual, or compel that individual to engage in some unwanted activity. Other communication devices, such as pagers or mobile phones, can achieve digital bullying.

II.6.6 Security incidents and cybercrime have to be reported

The number of security incidents reported to CERT [31] has been growing steadily since the start of the current century, as has the number of attacks reported to the legal authorities. This has contributed to a better understanding and accounting of computer crime. Large-scale police operations conducted in several countries have demonstrated that the authorities are reacting and adapting to the new criminal

[31] CERT Coordination Center, Carnegie Mellon University (http://www.cert.org)

context. The arrest and conviction of several virus authors and spammers testify to the determination of law enforcement officials to deal with these new types of nuisance. However, the number of convictions remains comparatively low, when considered in light of the sheer volume of spam and viruses circulating on a daily basis.

Few statistics have yet to be compiled regarding cybercrime - *most incidents go unreported*. Infractions tend to cut across borders criminal legislation tends to be national. It is difficult for authorities to compile statistics on crimes, because those crimes are defined differently from one country to another. Take, for example, the case of a computer system that is used to carry out a fraudulent financial transaction using a stolen user identity. This could be classified as either a computer-related crime or a financial crime.

The percentage of cybercrime that is actually reported is difficult to estimate. According to the Computer Crime Research Center, it may be less than 12% [32] in 2004. In 2008, some experts estimate cybercrime report around 20%. It is difficult to obtain a realistic inventory of computer-related crime. This is a serious obstacle to attempts to analyze the phenomenon and determine its magnitude.

The absence of official statistics is partly due to the fact that organizations:

- Wish to avoid publicity about attacks;
- May be unaware that they have been the victims of cybercrime, particularly in the case of passive attacks, such as the transparent hijacking of data, disrupting of traffic, passive listening, and undetected intrusion. They may also not learn of the attack until much later, when there is no longer any point in reacting;
- Do not know how to deal effectively with a crisis situation;
- Lack the necessary confidence in the legal authorities and police;
- Prefer to handle the matter themselves.

The precision, sophistication and potency of attacks and attack toolkits are constantly increasing. The quantity of attacks also continues to grow. The ever-increasing complexity resulting from this dynamic trend is difficult to handle. There is an urgent need for *strong political* will and a sense of responsibility among all participants at the international level, and effective partnerships between the private and public sectors. Otherwise, any security measures, whether of a technical or legislative nature, will wind up being inadequate, piecemeal, and ineffective.

More than ever, public authorities are called upon to play their traditional role of prosecuting and preventing fraud and crime. They also need to become active in educating and building awareness among the general public. In particular, it would be useful for public authorities to make available reference information on protecting persons and property during Internet use.

The protection and defence of an organization's assets needs to be organized, taking into account the risk of crime when defining the security strategy. It can be difficult to identify cybercriminals – not enough is known of their methods of action and their motivations. However, *criminal organizations* generally behave in an *opportunistic manner*, and tend to attack the most vulnerable targets. An organization can take steps to ensure that it is not an attractive target for cybercrime, by protecting its computer infrastructure better than its competitors, rather than contenting themselves with remaining on the same level of security.

By contrast, an organization that criminals view as a lucrative potential victim or an important symbol to destroy will inevitably draw targeted attacks. In the latter case, the threat of destruction by terrorist acts becomes a real possibility, which makes it essential to put an appropriate protection and defence strategy into place. However, conventional insurance and risk management tools are of limited effectiveness in dealing with the criminal risk. The only way to avoid certain risks would be to avoid connecting to the Internet altogether.

---

[32] Vladimir Gobulev, "Computer crime typology" published on 9 January 2004 by the Computer Crime Research Center: www.crime-research.org/articles/Golubev1203/

Cybercrime has a global dimension – one that affects organizations at all levels, including shareholders, executives, staff, and production facilities. Therefore, organizations must learn to safeguard their integrity in response to the risk of cybercrime, as they have learned to do with the risk of corruption. In order to remain profitable, they must compensate for the opportunity cost caused by cybercrime risk and the cost of measures put in place to manage it. Economists need to design an effective economic model that accounts for the costs of protecting infrastructure and providing security for systems, networks, data and services.

Conventional security measures based on a prevention-protection-defense approach regarding information assets and critical resources will be reinforced by using:

- High-quality products with a minimum level of security. “Safe products” should provide a manageable and verifiable level of security;
- Transparent and controllable security measures and tools.

In this context, security should not be the exclusive responsibility of users. All stakeholders have a security responsibility.

International authorities are faced with *synergies* and *convergence* in *organized crime, economic crime* and *cybercrime*. In light of that fact, they need to develop a comprehensive, multilateral and global response geared toward strengthening economic players' confidence in ICT and reducing the opportunities for crime.

This response must meet the imperative of ensuring the security of nations, organizations, and individuals. It must hold cybercrime down to an acceptable level; it must strengthen confidence in the digital world; and it should minimize the threat of corruption and destruction to the cyber world.

PART III

LEGAL, JUSTICE AND POLICE APPROACHES

Part III proposes legal, justice and police approaches related to cybersecurity and cybercrime issues. This part demonstrates the fundamental role of forensic computer techniques in cybercrime investigation and identifies some legal issues related to cybercrime and international cooperation that contribute to preventing, deterring and fighting cybercrime.

The Convention on Cybercrime (Council of Europe) is presented as an example of identifying areas of law to be addressed when dealing with e-activities. In addition, several legal aspects of cybersecurity which contribute to building a safer information society are analyzed. A discussion on privacy issues in the information society concludes part III.

III.1 COMPUTER FORENSIC

As outlined by *The World Summit on Information Society*, major society changes occur with the adoption of information and communication technologies. Evolution of the society generates for example changes in the way of committing crimes (technologies as a tool to perform criminal activities) and also to modify the target of crime (information, computers and telecommunication infrastructures become the object of illegal actions). The massive dissemination of tools for automated information's processing opened new opportunities to the criminals. They have learned how to exploit ICT vulnerabilities, knowledge and specialized tools, available on the Internet.

Criminals take advantage of the *aterritorial nature* of the Internet and the lack, in some countries, of legislation outlawing computer−related crime, as well as the multitude of jurisdictions covering the Internet. In a similar manner to monetary tax havens, digital safe havens allow criminals to host servers, distribute illegal content or perform illegal actions without fear of being brought to justice. Installing such servers on the territory of weak countries creates a haven for cross-border operations. The lack of international regulations and control, and the ineffective nature of *international cooperation* in legal investigations and prosecutions, allow cybercriminals to be very effective.

Furthermore, in most countries there is a significant mismatch between the skills of the criminals, who commit high−technology crimes and the resources of law-enforcement, and legal authorities to prosecute them. The use of computer technologies by these authorities, whether on a national or international level, varies greatly from one country to another but generally remains weak.

To prevent, deter and fight cybercrime, cyberthreats and cyberattacks should be well understood. *To pursue cybercriminals*, knowing cybercriminal motivations and their modus operandi is not sufficient, if the society is not able to supervise and recognize *illicit activities* and *discover criminals*. Therefore, trained persons, tools and procedures for cybercrime pattern recognition, tacking charge of digital evidence and performing computer investigations should be operational and effective.

III.1.1 Computer investigation and digital evidence

This section presents fundamentals in computer forensic and deals with the notions of crime scene, computer investigation, trace and proof in a digital world.

Any **criminal investigation** follows *procedures* developed in a specific appropriate framework. Some variations can exist from one country to another, but the following steps could be largely found: (i) research of indicators and clues, (ii) criminal identification and localization, (iii) tribunal evidence presentation.

When *law enforcement agents* are notified that a computer-related crime has been committed, police should *gather evidence of the illicit action*. As with any other criminal case, a *search warrant* may be executed; investigations, interviews or interrogations may be conducted in order to identify suspects and, if necessary, bring them before the courts. The purpose of any investigation is to discover and present facts that contribute to establishing the truth (Figure III.1).

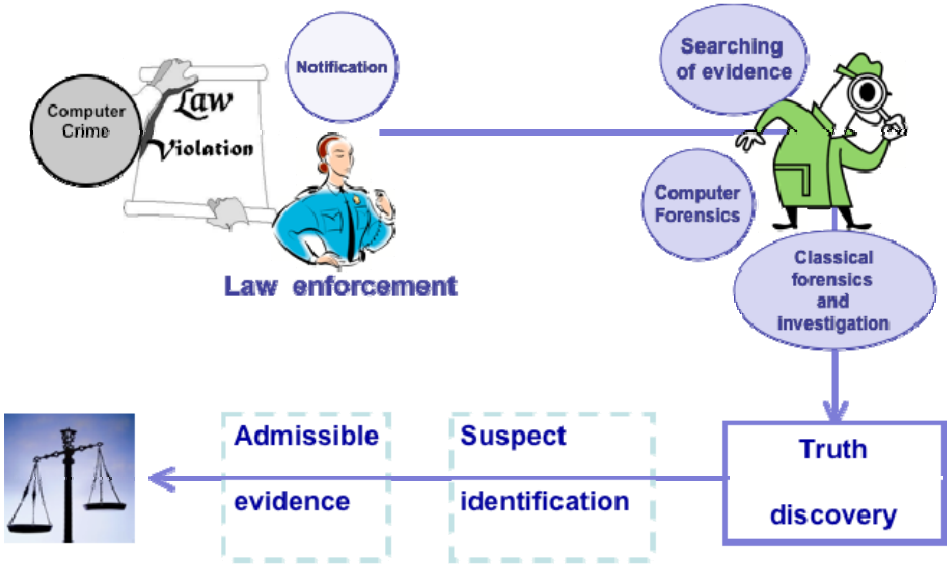

Figure III.1: Overview of a crime resolution process

The reasons for *conducting a computer investigation* should not be forgotten; the investigator must have knowledge of and respect legal procedures for handling evidence. If this were not the case, the results of the investigation could be compromised and thrown out by the court because of an insufficient or incorrect evidence-gathering process. *It is not enough to be a good computer technician; one must know the legal framework and constraints in order to perform a useful computer investigation.*

On a **computer crime scene**, police investigators and legal intermediaries must have received specific training. A *common vocabulary* between police force, justice and laboratory should exist. *Procedures* and strict rules for data-processing expertise should be set up in order to increase computer investigation performance and reliability. The resulting investigation *report* should be *easily comprehensible* and must describe in detail all the operations performed and procedures followed in order to gather digital evidence.

Investigators with a solid understanding of information technologies and the Internet, who use cybercrime investigation methodology in conjunction with effective international cooperation, could be able to uncover the criminal's identity. In most cases at present, the police and legal authorities rely on conventional investigation methods used for ordinary crime in order to identify, arrest and prosecute cybercriminals.

Digital information can help to validate or dismiss an alibi or a witness statement, to prove that a specific action was performed at a given time, to determine how a crime was committed, to reveal links between an offender and a victim, etc.

Which kind of information and where it can be found in the system and network, is mandatory knowledge for digital investigators? It means that they must understand how computers and networks work and be able to rely on appropriate methods and tools. But at the same time, a good computer technician is not necessary a good ICT investigator.

Any computer systems information and communication device (electronic components, memory devices, hard discs, USB sticks, etc.) or information it contains, are potential targets or instruments of

crime. Any devices are sources of digital evidence. Each software or data execution or transaction leaves digital traces in various components. For example, the traces left on a router can enable the remote system from which an attack was launched to be identified.

Digital evidence is even more difficult to obtain when it is scattered across systems located in different countries. In such cases, success depends entirely on the effectiveness of international cooperation between legal authorities and the speed with which action is taken. Effective use of such evidence to identify individuals depends on the velocity with which requests are treated: if the treatment is slow, identification is next to impossible. One of the most important features is the duration during which Internet Service Providers (ISP) keep information concerning user subscriptions and activities (IP addresses, connection data, etc.). The *retention period*, during which data is available in order to retrieve someone's identity from his IP address, varies from one country to another and can be decided by national law.

Legal systems must give law enforcement agencies the appropriate authority to access traffic data. The *legal constraint* of recording connection data for a certain amount of time (six months is a minimum, given the speed of international legal assistance procedures) obliges ISPs to provide adequate facilities to store and retrieve information when ordered. Countries should improve international cooperation and be able to share critical information quickly, otherwise digital evidence may disappear.

For Instant Messaging services and Peer-to-Peer or Internet Relay Chat facilities, logs and historical content of communications are kept for only a few days, when they are kept at all. In fact, there is no guarantee that logs or user records exist or are conserved. *Digital traces are volatile* and rapidly removed from servers, and anyone can run an Internet relay chat server, for example.

An IP address identifies a computer, not a person and criminals use false or stolen identities. It is always very difficult to establish the identity of a person on the basis of an IP address, email or web addresses or a digital trace. "**How can particular digital information be linked to its physical author**?" Once the IP address of a system involved in a criminal activity has been identified, the next step is to answer the question "*Who was using the computer*?"

III.1.2 Searching and collecting evidence

A trace is a mark, object or sign, not always visible to the naked eye, or a vestige of a presence or an action at place. Whatever the nature of the trace, one must ask the following questions when investigating a crime: *How was the trace made? Why is it present? Does its presence reveal an action that concerns the investigation?*

Within the context of cybercrime, *digital traces* may be seen as outwardly immaterial; nevertheless digital traces reside on a material reality – a particular state of memory (CD-ROM, etc.). Therefore, a digital trace is very similar to a traditional material one. *Any trace is fragile* and susceptible to deterioration; some may even be invisible or inaccessible. Consequently, the investigation of a crime scene comprising digital traces, requires a series of operations aiming at ensuring their potential quality as *evidence*. Intervening in a data-processing crime scene environment, necessarily implies applying the same general principles as on a traditional crime scene, such as the protection of places and documentation, selective research, etc. for example.

When searching for digital evidence, many problems arise, including these:

- Which elements may contain pertinent information for the case being investigated?
- How can the relevant data to be seized be identified?
- How to proceed?
- What are the procedure rules to be followed?
- How can data be collected, stored and preserved?
- How can data be safeguarded and proof, how it was collected, be established, so that it can be analyzed later on by other people?

- How can digital data be preserved as evidence for a potential hearing, knowing that the storage medium from which the evidence was recovered is not infallible (date-time information being treated differently from one computer system to another) and subject to tampering?
- How can data be copied from its support to another one in order to analyse it without modifying it?
- How can a non-modifying, “bit by bit” copy be performed?
- How can a copy be authenticated?
- How can the original data be preserved?
- How can it be guaranteed that the process of copying the data did not modify it?
- How can data copy analysis be conducted?
- How can files that have been deleted be recovered?
- How can a cybertrail be followed?
- How can the origin of a message be proven?
- How can an IP address that identifies a system in a network and an individual be associated?
- How can primary binary data be transformed into significant comprehensible information?
- How can results be presented to non-specialists?
- How can one avoid digital evidence becoming a false alibi?
- Etc.

To answer these questions, some *computer forensic tools* and *procedures* exist. They should be used by *trained and competent experts*. In the past few years, some evidence processing tools have been developed and commercialized, and their standardization is also an issue currently being taken into account.

On the other hand, criminals could be *tracked* by *active communication monitoring* and live surveillance. Telephone, e-mail or instant messaging eavesdropping is possible to collect information related to communication content or non-content such as e-mail headers or IP addresses. In fact, criminals can also be identified through undercover investigation when investigators join instant messaging (IM) services, peer-to-peer networks (P2P), Internet relay chat (IRC), newsgroups, etc. to lure criminals.

The chain of custody is a very important concept when dealing with investigation, forensic science, evidence and the execution of law. *It helps to preserve the integrity of evidence* in order to avoid that a legal representative of the defence can successfully argue that the evidence has been corrupted.

Like any material trace, a digital trace must satisfy certain criteria that make it possible to ensure its validity as a *means of proof* (authenticity, integrity). These criteria mainly include documentation of the trace and the history of the trace handling.

In a well documented report, the process of preserving integrity of evidence, or the way in which the custody chain is executed, must answer the following questions:

- Who gathered the evidence?
- How was the evidence collected?
- Where was the evidence found and amassed?
- How was the evidence stored, authenticated, protected and analysed?

- Who handled the evidence? From whom did he receive it? To whom was the evidence transferred?
- How is the evidence kept safe? How is it authenticated? How is it locked up? Who has access to it? Who took it out of storage and why?

III.1.3 Collecting evidence in cybercrime investigation

In *cyberspace*, it is difficult to define which way to follow when investigating an incident. Usual *computer investigations* are rather "host based" than "*network oriented*". An attacked computer, (mainframe, personal computer, or even a personal digital assistant (PDA), etc.) is scrutinised in order to collect traces of an offence. In the same time, a cybercrime scene should be seen as any other scene of crime with one further dimension, rather than a fully different space of investigation[33].

The very problem is the nature and kind of the trace to be collected in such a distributed systems' environment as the Internet. The trace can be a "traditional" one, like a fingerprint, but it can also consist in information characterising for example, some action that the targeted system is not supposed to perform. When a network is used, *traces are distributed all over interconnected systems*. This introduces a new level of *complexity* in the daily work of an *investigator who has to determine quickly which traces have to be privileged and where to collect them*.

The first question is to know what to look for. Three types of evidence can be valuable:

- The very evidence of the infringement's commission;
- The trace of an action, or a transaction made through one of the concerned systems;
- The link between a person and an act (since computer systems can be remotely controlled, the link between a person and a location is weakened when considered as a potential evidence).

There is often a *risk* to base the choice of which traces to look for in an emergency and crisis situation, on the first elements reported by the Information System Manager, who is usually the main interlocutor of the investigator. She/he has a constraint of business continuity that is not really compatible with the needs of an investigation. In fact, *she/he can also possibly be part of the malevolent act and have modified some traces in order to lead the investigator on a wrong trail!*

The "**human dimension**" must absolutely be taken into account, since it could jam the communication between both parties. As said by Alphonse Bertillon :"*One sees only what one looks at, and one looks at only what one has in the mind*". An investigator could be influenced by the traditional forensic way of exploring the scene of crime. At the same time, a computer scientist or an information system's manager has a totally different approach of the computer system and its environment. It is very important for the investigator to question these professionals keeping in mind their cultural grid.

The *relative value of the existing traces must also be evaluated* according to the life cycle of digital data. Finally, one must evaluate the *interest of discovered traces* through their possible value in a court, compared with the technical difficulties generated by their collection and conservation.

The notion of "**legal usability**" of a trace defines the easiness of acceptance of the trace by a court. It implies a strong reliability of the processes of finding, collecting, and of preservation of the trace. It should also mean for a digital trace that it has been created during the normal functioning of the system, rather than by a tool installed because of the occurring incident, and focused on it. This notion could be associated to her technical counterpart "**technical usability**", related to the level of specialisation required for the understanding and managing digital traces.

When dealing with cybercrime, the investigator has to locate the place and time of creation of the traces that could become potential evidences. This is particularly difficult since many actors can be involved at different moments of the criminal process, and geographically dispersed.

---

[33] Adapted from S. Ghernaouti-Hélie & al. "Evidence for cybercrime investigation" - poster –13th International Forensic Science Symposium -16-19 October 2001 - Interpol General Secretariat, Lyon.

Time location of digital traces could be classified according to the happening of the incident (before, during or after) as for example:

- *Before the incident*: exploration traces (scans detected); logs of connections from the attacker's IAP or ISP; "normal state" of the targeted system (traces created by a normal activity);
- *During the incident*: logs of the systems that could have been used, or targeted by the attacker; content of the swap files; dump of memories (RAM); system process management;
- *After the incident*: attempts of data modification, deletion or erasure, ("cleaning" traces or creating false traces); logs of current activity of the targeted system (can reveal rogue processes); manifestation of the attacker: claim (on Internet Relay Chat, forum, etc.), blackmail (anonymous mail…).

For the **space location** of relevant traces, the position of the author is not sufficient for the limiting of the area of investigation. An information system connected trough the Internet, can be distributed between many locations. For instance, when the server's management is outsourced, data are often stored on a server situated in a remote facility.

To reach this location, even from inside the company, a criminal would certainly use the infrastructure of an Internet Access Provider (or ISP). The physical support of the access could be different and each one of them will have its own policy for connections, logs creation and conservation.

Several space locations to look for digital traces could exist when dealing with:

- An usual computer investigation: traces are localised in a system ;
- A local area network (LAN) investigation: some network management tools can have stored information about the transactions or actions that occurred during the incident as for example:
    - Intrusion Detection Systems,
    - Firewall logs,
    - DHCP (Dynamic Host Configuration Protocol) servers,
    - Domain controllers (Windows environment),
    - Authentication servers,
    - Network load management tools,
    - Application servers (that could have been used during the crime's realisation),
- Internet environment investigation particularities: some of the "global carriers" (like backbone operators) log a lot of management information (in order to better manage their quality of service). This also can provide clues about the real attacker, or his/her true motivation.
- Internet Access or Service Provider (IAP / ISP) : Network management tools of the victim's IAP can be invaluable to find the origin of the attack (the "attacking system") and the possible destination of some of the stolen assets (specific data or financial transactions);
- On the other hand, the IAP / ISP of the attacking system gives information about
    - The time of internet access (when executed through ISDN or dial-up);
    - The amount of data exchanged and sometimes when the connection happened (on permanent connections like ADSL or cable); but this depends on the existence of the use of monitoring logs;
    - Logs of incidents;
    - Which Web pages (or sites) have been accessed, when a proxy is used and configured to keep a track of when the data stored have been retrieved.

In the forensic field, the *life cycle of a trace* is very important to be known, if one wants to avoid its destruction, or its contamination. For instance, investigators are used to handle biological traces in emergency, since most of those are often usable during only a short period. In the cyberspace, evidence can also be very "volatile".

Depending on the physical support and on the nature of the processes that created them, digital traces can be more or less resilient.

Four factors are determinant:

- The *easiness of creation*: this factor qualifies the technical difficulty encountered to create the trace during the normal operations of the system. It has a direct effect on the legal value of the trace, since a malevolent can create a false trace, or alter a real one when it is technically feasible;
- The *durability of the trace* on the support: this criterion helps to define on which kind of support the first investigations have to be led. The investigator must quickly make research on the media being the most volatile;
- The *speed of deletion* by the existing tools of the system: usually, the deletion of a file is easily performed by the operating system. But some applications (like database management systems, or journalised file systems) automatically clear all or part of the data. The deletion is therefore more complicated, since all images have to be treated. It is also important to be able to know when and following which conditional trigger, data are deleted by the normal activity of the system.
- The *ability to be fully erased*: some physical supports are very difficult to be cleaned. Specialised actions have to be performed if one wants to completely erase a trace from these supports. Even if magnetic storage devices are considered as sensitive to wrong use, most of the data they store are still recoverable after an incident.

Developing new ways of tracking evidences in cybercrime offences is becoming a necessity. By analogy, it has been previously the same when dealing with financial crime in the eighties. The apparition of new and complex financial tools, at the same time as the markets' globalisation, led to a growth of sophisticated financial crime. A considerable effort was conducted to teach judges and police officers how to investigate such affairs. Once seen as very "exotic", financial crime is now fully integrated in judicial mechanisms, and even if its investigation needs expertise, time and means, it is not seen as exceptional. In the same way, cybercrime is becoming more common and the judicial system should treat it easier, as more and more investigators and judges are taught how to deal with it and its peculiar traces.

To accelerate this evolution, methods should be developed to better qualify the incidents, and to help the investigator to engage enough resources when needed. Investigating a cybercrime can be time consuming, and focusing on the right source of traces can become the only way to lead a case to its achievement. Another improvement could be the collaboration between the investigator and the people in charge of ICT infrastructures and security, who are concerned by the offence. This can be notably improved in perceiving the *investigator* as "*computer literate*" or *technically competent* by in system administrators in place. Two ways lead to such a professional recognition: training and formalisation. *Training is a question of human resources management.* Formalisation is the consequence of applied research. By comparing best practices and existing guidelines with what is really needed in the field by the officer as well as joint methods of cyber scene crime investigation, could improve and develop the investigator's efficiency, helping to be accepted by professionals.

III.1.4 Computer crime investigation methodology

In the same way criminals have developed *attack methodologies and patterns* that can help them to be efficient, investigators should learn to optimize computer crime investigation by transferring practical knowledge into *rigorous search strategy methodology* and *standard operating procedures* (Figure III.2). Before starting on a case, an investigator has to carefully *prepare* his methods.

Following a specific *methodology* is always beneficial and allows essential actions not to be omitted, in order to reach reliable and well-documented conclusions.

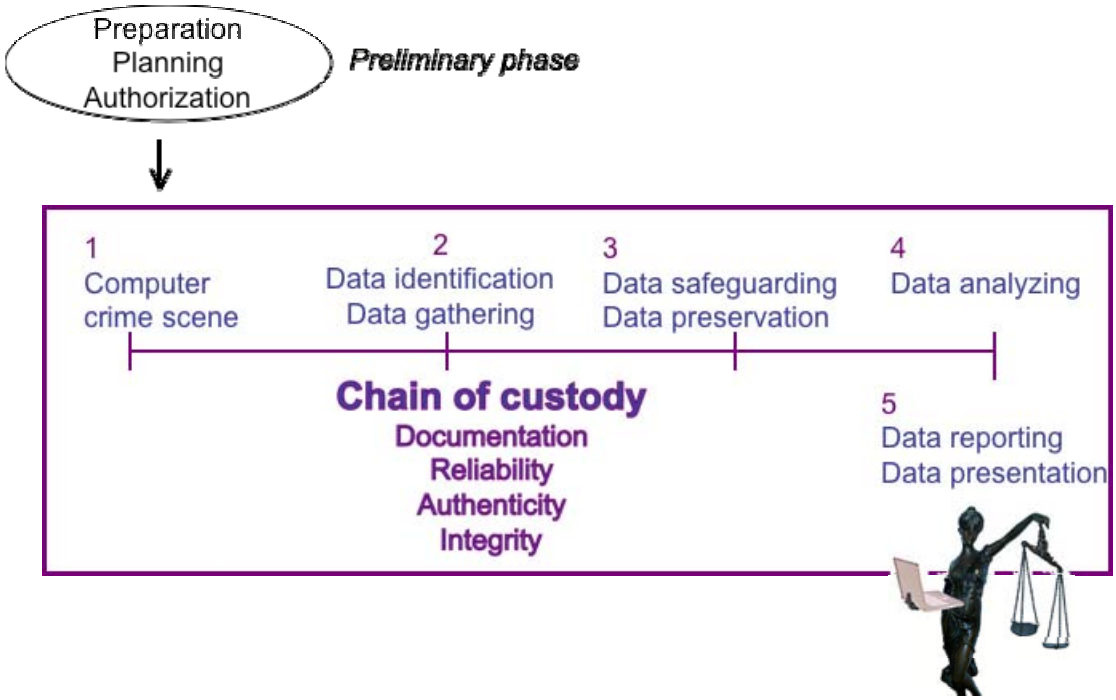

Figure III.2: Computer crime investigation methodology

The aim of the preliminary phase is to gather information about the place and ICT environment to be investigated (line of business, ICT resources and infrastructure, type of data, of systems, aim of the investigation, tools and skills required to intervene, etc.).

Phase 1 should be to freeze the scene of crime in order to prevent the ICT context from being modified before digital traces are collected, and to avoid giving the malicious person a chance to modify or destroy evidence. The goal of phase 1 is to avoid the destruction or the dislocation of crucial data. This means interrupting activities in progress and moving people away, in the same way in which yellow bands set the limits of a traditional crime scene. To prove the state of data at the time of intervention, data should be fixed in a reliable way before being manipulated. This is similar to taking photos or videos of a traditional crime scene.

The identification of relevant material in which data may be found and preserved can lead to specific hardware being removed from the crime scene, bearing in mind that complete seizure is not always possible or relevant. The investigator must classify resources to determine which system must be removed from the scene using the proportionality principle (importance of the relevant material for the crime committed, versus the importance of the potential nuisance for the owner, if it is taken away).

Identifying traces and collecting them comprises the second phase (*phase 2*), and this should be followed by the data safeguarding and preservation phase (*phase 3*). At this stage, data can be analyzed (*phase 4*) and subsequently presented in a comprehensive way for non-experts (*phase 5*).

To investigate a computer crime within an information system of an organisation, it is consequently important to define the procedures to be implemented if one wishes to improve the collaboration

among investigators and responsible persons for information technologies security, in order to *facilitate the identification's work of the perpetrators by the justice*[34].

III.1.5 ICT security manager and ICT police investigator collaboration

Quality, know-how, different constraints and objectives are at the *origin of numerous lacks of understanding* between an investigator and an ICT security manager. The risk is big to see these differences becoming real obstacles to the proper functioning of the investigation.

Whereas the *ICT security manager* tries to recover its systems in the briefest time, to ensure the continuity of the production, the investigator is subjected to the formal constraints of the penal procedure, which requires from him to obtain as much traces as possible, and to preserve them in accordance with very precise legal standards.

The concern of reactivity of the *ICT security manager* is going to incite him to concentrate on the means needed to *stop the aggression and limit its impacts*. The problem of identification of the author is for a security manager, secondary towards the preservation of the activity of the organization. So the recovery of the system represents for him the end of the incident while it is often situated at the beginning of the *investigator*'s intervention (*temporal gap*).

The procedures of reboot (*restart*) of an information system are often contradictory with the conservation of traces which would allow *proving the reality of the attack*, to select a group of suspects, and to *obtain possible legally valid evidences*.

Furthermore, this gap can also be widened by certain behaviours of an ICT security manager or a system administrator, if they try to resolve the crime by themselves. They possess generally a partial knowledge of the legal constraints consecutive to the conducting of a penal investigation. They usually are not experienced in the correct management of existing traces. Besides, their different attempts will also have the effect of delaying the implication of the police forces and in many cases, awakening the attention of the offender. Furthermore, they can be actively involved in the criminal process. All this will generally have the effect of slowing down, and even hindering, the progress of the investigation.

On his side, the investigator has most often an insufficient vision of the technological, organizational and human context of the concerned institution.

A certain number of obstacles to the smooth functioning of the investigation are added because cybercrime also leads, besides the damages provoked directly by its commission, to an erosion of the image of the attacked organization, which consequently implies a low level of denunciation of the computer offences. Furthermore, the negative image sometime associated to the supposed weakness of the investigator's technical knowledge, strengthens the hesitation to report officially the undergoing attacks. The perception of a relative incompetence is strengthened by the real lack of communication strategy on these subjects on behalf of the police forces.

To be effective, the collaboration between police investigators and security managers, will have to be based on a certain number of points that can't be ignored by the involved parties. It is not possible to envisage the *reduction of the cultural and technological gap* separating policemen and system's administrators (or security managers) without underlining the mandatory, inevitable character of their collaboration in case of investigation. It should be based on the understanding of each one's objectives, and the recognition of the importance of the temporal constraint in the management of their collaboration. It means in particular that the human dimension of this interaction should be privileged. The technological aspect should remain a support for the action.

Among *practical measures*, we can quote some examples:

- Logs should be protected and authenticated;
- Backup supports for log files should not be rewritable;

[34] Adapted from S. Ghernaouti-Hélie & al. "Pursuing Computer Crime within an Organisation: a Matter of Collaboration between the IT Security Manager and the Investigator". Second European Academy of Forensic Science Conference. Cracow, 12 -16 September 2000.

- The format of these files should be as universal as possible;
- The place where backups are stored should be protected;
- Duration for backup storage should be long enough;
- The risk analysis performed during the elaboration phase of the security policy should lead to the definition of quantitative parameters, allowing the measuring of how critical the different log files are;
- Security policy should be implemented and managed by skilled professionals;
- Practical measures should be an integral part of the specifications of the security policy;
- Etc.

III.2 THE LEGAL DIMENSION OF CYBERSECURITY

III.2.1 Needs for a legal framework

ICTs allow huge amounts of information to be stored, processed, accessed, searched, transmitted, exchanged and disseminated, regardless of geographical distances. These unprecedented possibilities could lead to new services that would improve economic development and widespread knowledge. On the other hand, new types of crime have appeared, and old types of crime are now being committed by using new technologies. While technical and managerial security measures have to be effective, a legal framework has to be put in place in order to prevent and deter criminal behaviour and to protect the citizen.

Cybercrime is not restricted by geography or national boundaries. A criminal located in one country can commit a cybercrime that produces its effects in a different country. Domestic laws are confined to a specific territory, but electronic exchanges or data flows do not know any geographic boundaries. In this context, a national cybersecurity and cybercrime legal framework should be enforced on a national level and compatible on the international level.

The need to build an appropriate legal framework for the use of new technologies leads to the drafting of many new laws. However, in this whirlwind of new laws it is important not to lose sight of the fact that much of the previously existing legislation applies to cyberspace - **What is illegal "offline" is also illegal "online".** The economic value of the investments needed for the guarantee of a minimum level of security (physical and legal protection) varies, depending on the organization's potential material losses and risks to its reputation and image. Legislation can be seen as an endogenous factor of security.

III.2.2 Convention on cybercrime

The Convention on cybercrime (*ETS n°185*) was adopted by the **Council of Europe**, on November 8, 2001. The 11/8/01 Convention and its Explanatory Report, were proposed for signature on November 21, in Budapest on the issue of the International Conference on Cybercrime. Today this convention is a reference document that has acquired worldwide recognition. The 11/8/01 Convention aims to create a common criminal policy against cybercrime by adopting appropriate legislation and boosting international cooperation.

The convention identifies cybercrimes that should be prosecuted and gives directions for the investigation of such crimes. The problem of international cooperation is also addressed. The Convention on Cybercrime of the Council of Europe can be seen as a starting point when studding the legal dimension of cybersecurity. The convention will be briefly discussed hereafter, in order to draw guidelines, developing countries could take into consideration in their national legal frameworks for fighting cybercrime. A typology of laws is also proposed as a general reference to guide nations in identifying their cyber security legal needs.

III.2.2.1 Overview

Chapter I of the 11/8/01 Convention contains a brief *definition of terms*. Chapter II defines *measures that are appropriate to the national level*. Chapter II, Section 1 deals with *substantive criminal law*; Section 2 deals with *procedural law*; Section 3 deals with *jurisdiction*.

The following four categories of offences are presented in Section 1:

- Offences against the confidentiality, integrity and availability of computer data and systems (Title 1);
- Computer-related offences (Title 2);
- Content-related offences (Title 3);
- Offences related to infringements of copyright and related rights (Title 4).

III.2.2.2 Criminal Law

Chapter II, Section 1 of the 11/8/01 Convention presents four categories of offenses that are to be subject to criminal law.

Section 1, Title 1 concerns offences against the confidentiality, integrity and availability of computer data and systems. Title 1 singles out the following types of transgressions:

- Illegal access (Article 2);
- Illegal interception (Article 3);
- Data interference (Article 4);
- System interference (Article 5);
- Misuse of devices (Article 6).

Section 1, Title 2 concerns computer- related offences. Title 2 makes the distinction between:

- Computer related forgery (Article 7); and
- Computer related fraud (Article 8).

Section 1, Title 3 concerns content-related offences. Title 3, Article 9 deals with offences related to child pornography.

The additional protocol to the convention on cybercrime (EST 189) concerns the criminalization of xenophobic acts committed via computer systems. It reads as follows:

> "Racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

The following activities, in addition to aiding and abetting, are punishable: dissemination of racist and xenophobic material through computer systems, racist and xenophobic motivated threats, racist and xenophobic motivated insults, denial, gross minimization, approval or justification of genocide or crimes against humanity.

Section 1, Title 4 concerns offences related to infringements of copyright and related rights (Article 10).

Section 1, Title 5 concerns ancillary liability and sanctions. Title 5 deals with the following issues:

- Attempts to commit, and aiding or abetting (Article 11)
- Corporate liability (liability of a legal person) (Article 12)

Article 13 concerns Sanctions and measures. This relates to consequences flowing from the serious nature of these offences by providing for criminal sanctions that are effective, appropriate and dissuasive. It reads as follows:

> "Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions."

III.2.2.3 Procedural Law

The explanatory report on the 11/8/01 Convention on Cybercrime introduces Chapter II, Section 2— Procedural Law as follows:

> "The articles in this Section describe certain procedural measures to be taken at the national level for the purpose of criminal investigation of the offences established in Section 1, other criminal offences committed by means of a computer system and the collection of evidence in electronic form of a criminal offence. In accordance with Article 39, paragraph 3, nothing in the Convention requires or invites a Party to establish powers or procedures other than those contained in this Convention, nor preclude a Party from doing so."

Section 2 presents five categories of procedural issues. It begins with two general provisions that apply to all of the articles relating to procedural laws.

Section 2, Title 1 concerns common provisions (Articles 14 and 15).

Section 2, Title 2 concerns expedited preservation of stored computer data. Title 2 makes a distinction between the following two types of data:

- Expedited preservation of stored computer data (Article 16);
- Expedited preservation and partial disclosure of traffic data (Article 17).

Section 2, Title 3 concerns production order (Article 18). A "production order" provides a flexible measure that law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

Section 2, Title 4 concerns the search and seizure of stored computer data (Article 19). Its aim is to modernize and harmonize domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural legislation includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data.

Section 2, Title 5 concerns real-time collection of computer data. It makes a distinction between the following two types of data:

- Real-time collection of traffic data (Article 20):
- Interception of content data (Article 21).

Title 5 addresses the problem of data collection by law enforcement authorities and by service providers. It also deals with obligations of confidentiality.

The section "jurisdiction" states that each party is required to punish the commission of crimes that are committed on its territory.

Chapter III of the 11/8/01 Convention presents the following: (i) principles related to international cooperation, extradition and mutual assistance; and (ii) procedures pertaining to mutual assistance requests in the absence of applicable international agreements.

Article 35 states that existing police cooperation and mutual assistance modalities need a point of contact available in each country 24 hours per day, 7 days per week, in order to ensure immediate assistance in investigation.

III.2.3 Some law domains related to cybersecurity issues

Chapter One of the ITU Global Cybersecurity Agenda addresses legal measures and an inventory of relevant instrument related to computer crime[35]. Figure III.3 summarizes common types of computer and data related offences identified in this document.

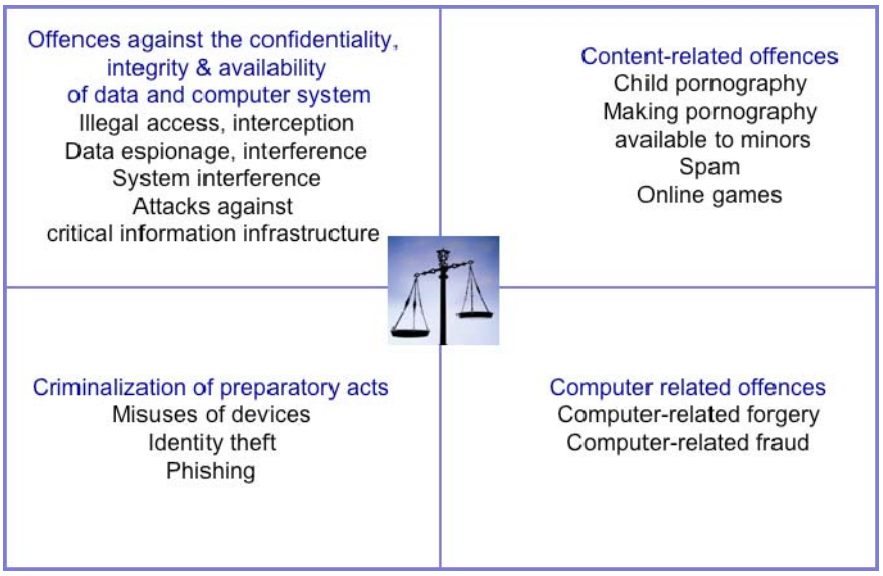

Figure III.3: Some computer and data related offences

In order to criminalize cybercrime, developing countries should adapt their legislation's domains. It is inconceivable to come up with an exhaustive list of law domains, mainly because:

- Countries may have substantially different legal structures and terminologies;
- Countries may have substantially different definitions of cybercrime;
- Laws must be adapted to the dynamism of technology evolution.

The following is a non-exhaustive list of proposed law domains: (i) Penal; (ii) Civil; (iii) Commercial; (iv) Telecommunication; (v) Privacy and data protection; (vi) Copyright; (vii) Unfair competition; (viii) Banking and professional secrecy; (ix) Right of disclosure/access; (x) Statuary obligations for storage/disclosure; (xi) Accounting.

[35] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

III.3 SOME E-COMMERCE RELATED LEGAL ISSUES

E-commerce can be discussed from the following two distinct points of view: (i) electronic business conducted with consumers - business-to-consumer (B2C); or (ii) electronic business conducted between companies - business-to-business (B2B). This is an important legal distinction because commercial law tends to differentiate between transactions between companies and those with consumers.

In either situation, security together with sound Internet marketing and sales tactics, conducted in compliance with an appropriate legal framework, is the cornerstone of e-commerce. By instilling *trust* based on security tools and respect for the law, countries can create a context that is conducive to the exchange of data. This will encourage the general public to adopt information technology and telecommunication services and at the same time develop a true service economy.

Because cyberspace is an international and transborder space, it is difficult to pin down, who has jurisdiction to resolve the legal issues arising from e-commerce. This is why Internet transactions must specify the offer's limits, and provide accurate information regarding which courts have jurisdiction in the event of a dispute.

Personal data protection is a key aspect of e-commerce. Consumers have a right to be informed about the nature of the data collected, used and communicated by online advertisers and businesses. They should know beforehand how the data concerning them is to be used and communicated, and who else will have access to it. They should also be told what steps will be taken to protect that data. An effective privacy policy must be clearly expressed, easy to locate and consult, transparent and comprehensible when the business transaction takes place. It must be posted on the company website.

The **confidentiality** of personal data and **digital privacy** are **fundamental human rights**. A number of such laws already exist, and companies have to take them into consideration when providing e-commerce services.

Since the early 1970s a number of countries have adopted *national legislation on personal data protection and control* of the use of public records containing nominative information, in order to prevent personal data from being stored unnecessarily or improperly. An European directive on these issues has existed since 1995 (Directive 95/46/EC of October 1995).

Legislation of this kind usually contains provisions relating to the following issues:

- Definition of nominative or personal data;
- Rights of access, objection and correction;
- Purpose of the processing;
- Data collection, storage and updating;
- Security of nominative records;
- Sale of data;
- Monitoring of crossborder data flows.

All persons have the right to be protected against abuse of personal data, irrespective of the medium and technology used to collect and process the data. Personal data can be defined as all information related to an identified or identifiable person.

The first legal problem posed by e-commerce is how to define the geographical area within which the electronic transaction takes place. Characteristics of the Internet such as international coverage, digital technology, and mode of operation are incompatible with the concept of geographical state borders. Information flows do not stop at international frontiers.

Regardless of where the Internet users and servers are located, data and services are accessible and can be provided remotely. Seller and customer are often transacting from within different countries. Therefore, a key point of any transaction is *to establish which nation's law is applicable* in the event

of a **dispute**. It is essential that transactions carried out over the Internet, indicate the offer's limits and provide specific information on which courts have jurisdiction in the event of a dispute.

The *contracting parties* may agree on a choice-of-law and court of jurisdiction. In the absence of a choice of-law clause, it has to be determined whether the contract comes within the scope of: (i) an international treaty such as the Unidroit Principles of International Commercial Contracts (1994); (ii) a form of netiquette; or (iii) The Hague Convention of June 15, 1955. International treaties are not binding, unless they have been expressly incorporated into the contract. If none of these solutions is possible, the rules of contract law apply.

The rules applicable to contracts concluded electronically are generally the same as those that apply to so-called traditional contracts. A contract has been concluded when one party has made an offer and the other party has accepted that offer.

For example, Directive 97/7/EC of the European Parliament and the Council of Europe, of May 20, 1997, deals with issues of distance sales and e-commerce. It stipulates that in good time prior to the conclusion of any distance contract, the consumer shall be provided with the following information:

a) The supplier’s identity and, in the case of contracts requiring payment in advance, the supplier’s address;

b) The main characteristics of the goods or services;

c) The price of the goods or services, including all taxes;

d) Delivery costs, where appropriate;

e) The arrangements for payment, delivery or performance;

f) The existence of a right-of-withdrawal, except in the cases referred to in Article 6 (3) of the Directive;

g) The cost of using the means of distance communication, when it is calculated at other than the basic rate;

h) The period for which the offer or the price remains valid;

i) In the case of contracts for the supply of products or services to be performed permanently or recurrently: the minimum duration of the contract, where appropriate.

The most important point concerning the conclusion of the contract relates to the *definition of what constitutes* an "*offer*" and *what constitutes* "*acceptance of an offer*".

The directive considers that a firm offer has been made, and the contract entered into, when the buyer accepts or clicks on "*Purchase*". Intent to buy is not expressed merely by visiting a site, any more than it would be by entering a shop. The display of goods on a website constitutes an offer only if the seller indicates the stock on hand and that stock decreases subsequent to the order, or if the nature of the goods is such that the seller is always in a position to fulfil the order.

The contract is concluded once the recipient of the service, i.e. the consumer wishing to purchase the goods displayed, receives electronic confirmation from the seller. However, that applies only if both documents are sent within a short time of each other. Thus, the 5/20/97 Directives make a distinction between a contract that becomes known to both parties at the same time and one that does not.

Certain conditions must be met in order for an **electronic signature**[36] to be considered to have transposed the handwritten signature on a paper document into the digital world. These are the following: (i) it must be uniquely linked to the signatory; (ii) it must be capable of identifying the signatory; and (iii) it must be created using means that the signatory can maintain under his sole control.

For example, Directive 1999/93/EC of December 13, 1999 on a European framework for electronic signatures distinguishes between three types of electronic signature *depending on the* degree to which

[36] Electronic signature mechanism is explained in part IV of this document.

the encryption mechanisms have been integrated and *the level of security afforded*. A key concern is that it is possible for a message to simply be "signed' without the signature being linked to the content of the message. In this case, anyone could "detach" the signature from the message and use it in the place of the signature's rightful owner. To overcome this shortcoming, a cryptographic function can be used to link the signature to the content of the message and to validate the sender's authenticity and the message's integrity on reception (concept of advanced electronic signature). The 12/13/99 Directive also discusses secure electronic signatures, which are based on the security provisions of Annex II on requirements for certification service providers issuing qualified certificates.

The ease with which items can be bought on the Internet can induce some consumers to act hastily. In this context, the **right-of-revocation** is especially important.

In the European Union for example, the right–of-revocation is regulated by Directive 1997/7/EC of May 20, 1997. The 5/20/97 Directive stipulates that for any distance contract the consumer has a period of at least seven working days in which to withdraw from the contract without penalty and without giving any reason. The grace period if three months if the supplier has failed to fulfil the obligations laid down in Article 5, in particular as concerns the conditions and procedures for exercising the right-of-withdrawal.

Those involved in a dispute arising from a validly concluded contract will have to furnish evidence, whether the contract was concluded electronically or not. Therefore, it is always advisable to keep a record of the transaction, such as a copy of the electronic message or a screen print.

Because of the international nature of e commerce, policymakers have devised means for resolving disputes that bypass the traditional courtroom. The concept of **Online Dispute Resolution** (ODR) was born of the desire to find immediate solutions to the non-performance of contracts concluded over the Internet. Conciliation is the basis of this type of dispute resolution: it involves negotiation, mediation and arbitration. It is quicker, cheaper and more convenient for the users. The drawback is that it is based on codes of conduct and recommendations, also known as soft law. This makes it difficult to enforce decisions. A good example of these codes is ICANN's Uniform Domain-Name Dispute Resolution Policy.

III.3.1 Cyberspace and intellectual property: some basic considerations

Intellectual property rights are protected by several branches of law. These include:

- Trademark law;
- Copyright law;
- Patent law;
- Design and model law;
- Laws protecting plant varieties;
- Laws on semiconductor topographies;
- Laws on public coats of arms and other public signs.

Laws on unfair competition also affect intellectual property rights.

Copyright law protects the following:

- Authors of literary and artistic works;
- Performers, producers of phonograms or videograms and audiovisual communication enterprises.

This branch of law defines a “work” as a creation of the literary or artistic spirit; it is individual in nature, no matter what its value or intended purpose. Creations of the literary or artistic spirit include:

- Works that use language, be they scientific, literary or other;

- Musical and other acoustic works;
- Works of fine arts, in particular sculptures and graphic works;
- Works with a scientific or technical content, such as designs, plans, maps, or sculpted or modelled works;
- Architectural works;
- Works of applied arts;
- Photographic, cinematographic and other visual or audiovisual works;
- Works of choreography and mime;
- Computer programs (software);
- Projects, titles and parts of works that are individual in nature.

The “author” is defined as “the physical person who created the work”. In the event that authorship is in question, the “presumed author” is defined as “the physical person who brings out the work until such time as the author has been designated”. Copyright entitles the author to moral and proprietary rights.

Copyright is considered to exist as soon as the work in question is created. It is not necessary to deposit the work with an office or to register the rights, although some countries do have copyright deposits. However, creating a work is one thing. Proving that one has created that work is another. The point is that the burden on the author is not to register the work, but rather to be able to prove actual authorship. Ideas cannot be protected unless they are set down because only the tangible work can be protected.

"*Moral rights*" refer essentially to recognition of authorship and to the right to decide whether, when, in what way and under what name the work can be released. "Proprietary rights" relate to the actual use of the work. i.e., production and sale of copies, presentation, distribution, broadcast, etc.

Transfer of ownership of the work, whether a copy or the original, does not imply transfer of copyright. Copyright is assignable and inheritable.

"*Neighbouring rights*" refers to the rights of performers of phonogram or videogram producers and of audiovisual communication enterprises. In this context “performers” is defined as “the physical person who perform a work or who participate artistically in its performance”. Neighbouring rights allow a musician to protect a particular recorded performance of a particular musical work. The actual musical work itself may very well have been written and copyrighted by a different individual. For example, a pianist may protect his performance of a piano work composed by Chopin or Beethoven.

The purpose of a **trademark** is to distinguish the products and/or services of the trademark owner from those of other companies. The trademark identifies an object rather than a subject of law - an object that tends to be identified by a name or a company name.

It is not possible to obtain trademark protection for the following:

- Signs that are in the public domain;
- Forms that correspond to the nature of the product or that are inherent to its use;
- Misleading marks;
- Marks contrary to the law in force or to the principles of morality.

The company or individual must register the mark in order to benefit from protection. The validity of a registered mark may be challenged.

The following are reasons why the registration of a mark might be revoked: (i) It is identical to a mark previously registered for an identical product; (ii) It is identical or similar to a mark previously registered for similar products and/or services and there is a risk of confusion.

Patent laws apply to for industrial inventions. Patents cannot be obtained for the following: (i) obvious by-products of technical developments; (ii) plant or animal varieties; or (iii) the biological processes used to produce plants or animals. Patents can be obtained for microbiological processes and the products obtained using such processes.

The patent may be granted (under specific conditions) to the inventor, his successor in law, or a third party who owns the invention on other grounds. If several people invent the same product or process independently, the patent is granted to the person who files first, or whose filing has priority.

The protection of the intellectual property of a website involves several branches of law. The registration of the domain name does not as such confer any specific exclusive right to the owner. Those rights are procured through the following legal bases:

- Trademark law;
- Laws governing company names;
- Laws governing the right to a name;
- Competition law.

Regarding the content of the site, and specifically the distribution of works via the Internet:

- If the content was created specifically for the site, it is protected by copyright;
- The digitization of an existing work and its online distribution are a form of reproduction that requires the consent of the author of the original;
- In the case of links to other sites, the use of a simple hyperlink infringes no exclusive right since it involves no reproduction. Deep links, which direct the user to a specific page within another site and bypass the site's home page, are another matter. The issue is whether or not the page in question is considered to be a work. As a rule, questions like this are regulated by competition law. The decisive criteria are the way in which the hyperlinks are used. Fair use is a key concept here.

Policymakers are introducing technical measures to ensure respect for copyright. They are enacting legislation to ensure that those measures will not be circumvented. Copyright thus enjoys legal protection, technical protection, and legal protection of the technical protection.

III.3.2 Some legal considerations related to spam

Broadly speaking, spam refers to the sending of unsolicited messages. Its characteristics are as follows:

- The unsolicited messages are sent en masse, over and over;
- The messages have a commercial purpose or are malicious in intent. Examples of the latter include phishing, taking over the computer, or introducing insidious software such as viruses, adware, and spyware;
- Usually the addresses have been obtained without the owner's knowledge, in violation of the rules relating to the protection of personal data;
- Often the content is illegal, misleading or harmful.

Spam is covered by several branches of law in particular data protection and unfair competition law; spammers also incur criminal liability.

Spamming, can be seen as a particularly *aggressive sales method*. There is no legal framework specific to advertising on the Internet, but the advisory opinion held that advertising on the Internet should be subject to a number of basic rules, whether it is used to conduct "traditional" business or e-commerce, as for example:

- The protection of young Internet users;

- Respect for the human being;
- Respect for fair, truthful and honest advertising;
- Respect for the legal privacy of Internet users;
- Ease of navigation.

"*Unfair competition*" occurs in particular when someone:

- Provides inaccurate or fallacious information on himself, his business, his company name, his products, his works, his services, his prices, his inventory, his sales or business method or, by providing such information, provides a third party with an advantage over their competitors;
- Displays or uses inaccurate titles or occupational designations of a kind to make others believe he has certain distinctions or capacities;
- Takes measures of a kind to lead to confusion with another person's merchandise, works, services or business.
- Hampers the customer's freedom to decide by using particularly aggressive sales methods.

When spammers act with *criminal intent*, they incur *penal responsibility*. Even if their message is commercial in nature, the content can lay them open to prosecution.

A majority of spam messages invite the reader to visit *pornographic sites*. In some country, as Switzerland for example, this is a criminal offence (article 197 of the Swiss Penal Code). It is considered a particularly grievous offence under the following circumstances: (i) the message makes the content available to people who do not wish to receive it; or (ii) the message is targeted to persons under the age of 16. Always as an example, the Swiss Penal Code defines fraud as activity intended to obtain a financial advantage from the victim for the purpose of self-enrichment. Seen from this angle, the "Nigerian letter" spam certainly qualifies as fraud. Spam is the chosen method of many criminals who infect machines with viruses. If the introduction of a virus results in data corruption, the spammer can be prosecuted. If the victim's data are modified, erased or rendered unusable, it is considered to be data corruption. Swiss law also prohibits the use of spam to sell medicines (advertising that encourages excessive, abusive or inappropriate use of medicinal products; and advertising for medicinal products that cannot be sold on the Swiss market or are obtainable only by prescription).

There are two opposing methods of *regulating spam*: the opt-in approach and the opt-out approach.

The *opt-in approach*, which is also called permission marketing, is more respectful toward the Internet user. It permits the sender to send only the targeted advertising that the recipient has explicitly agreed to receive (by selecting a box on the screen). Agreement may also be inferred, but in that case the visitor must be clearly informed of the commercial nature and of the consequences of subscription.

Under the *opt-out method*, every advertisement sent must give the recipient the option of “unsubscribing” from the list. The opt-out method establishes the right to refuse to receive messages “à posteriori”. Opt-out records can be constituted lawfully (for example by buying an opt-in list) or harvested using a random procedure.

The European Union tends to favour the opt-in approach. For example, the European Union’s Directive on privacy and electronic communication (Directive 2002/58/EC) uses the opt-in method. This directive concerns the processing of personal data and the protection of privacy in the electronic communications sector.

Because spammers tend to act anonymously and from abroad, litigation is expensive and complicated, and usually involves engaging a lawyer.

Because legal remedies alone have little impact on the spread of spam, a technological solution is required. Only by using technical and legal means together can the phenomenon of spam be combated effectively. Every spammer who is discouraged by a rule of law or effectively prevented from spamming by a technical solution, means millions and millions of unsent messages.

The impact of spam can be limited by using technical means to restrict: (i) the number of recipients per message; (ii) the number of messages per source; and (iii) the number of messages per unit of time.

Blacklists work on the principle that mail can be classified using the server's reputation as a criterion. The reputation of a mail server that has recently delivered spam is tarnished as it can be assumed that the server will send more spam in the future. The server can be identified by its IP address.

Key word filters block messages containing certain key words. They are ineffective because spammers can easily compose their messages to get around the filters.

Profiling technology makes use of a database of contents that has been identified as spam. The technology is used to profile the content of a given message and compare it to a database of contents considered to be spam.

A growing variety of "malware" (viruses, Trojan horses, bots, etc.) is being used to install e-mail servers on infected machines. The aim is to make it easier to propagate spam. Therefore, an important aspect of *fighting spam* is to *hunt down malicious software*.

Anti-spam software can help filter and block spam at the level of the e-mail server and thus limit its spread, but it is not always effective. Legitimate messages do not always reach recipients and genuine spam is not always filtered out.

User attitude is a key aspect of the fight against spam. The scope of the problem can be limited if users treat messages knowledgably. That includes the following: (i) being aware of the risk of identity theft; (ii) checking what use will be made of their e mail address before divulging it in an online form; (iii) using several e mail addresses; (iv) avoiding certain types of sites; (v) never opening messages from unknown senders; (vi) deleting spam without reading it; (vii) never replying to spam; and (viii) never clicking on the hyperlinks in a spam message.

III.3.3 Summary of the main legal issues relating to cyberspace

The *legal issues regarding e-mail* are: (i) message content; (ii) mailbox address; and (iii) identity theft, including the theft of a distinctive sign or a company name. These points are regulated by each country's civil law.

The *legal issues regarding websites* are: (i) copyright issues centring on the definition of a “work”; (ii) questions of content, responsibility, and protection related to hyperlinks; and (iii) questions relating to search engines.

In addition to the many legal issues involved, *contracting in cyberspace* raises challenging technical issues. What technical mechanisms will be used for actually concluding a contract? What specific tools and procedures will be used? How can policymakers contend with global impact, intangibility, and delocalization that defines cyberspace? The following issues are important from the legal point of view: The offer; its status (whether or not it is distance); what constitutes its acceptance; Advertising and soliciting; spam; etc; Performance; Online acceptance of the offer and the information technology used to indicate acceptance; The right-to-withdraw; Choice of law and jurisdiction.

Contracting Electronic documents that are signed electronically raise issues of validity. The aim is to be able to guarantee the legal validity of the signature in order to identify the signatory and to ascertain that he intended to sign the document and therefore takes responsibility for the content.

The danger with *electronic payments* involving credit cards, cheques or electronic money is the risk of being intercepted by third parties and the relevant information misused. When the service supplier and the recipient communicate, they are vulnerable to this type of interception.

Domain names are a new form of intangible asset that can have considerable commercial value. Policymakers need to assess this issue from the following points of view: (i) Trademarks and domain names; (ii) Distinctive signs; (iii) Business names and domain names. The US Anticybersquatting Consumer Protection Act (ACPA) is a major piece of legislation that tackles these issues.

Contracting Electronic *Intellectual property* on the Internet raises issues relating to copyright, trademarks and patents. A legislative initiative concerned with these issues is for example the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

Contracting Electronic Spamming is an infringement of the *right to digital privacy*.

Many other legal issues have to be considered when defining an appropriate legal framework for use of the Internet as for example antitrust legislation, the liability of suppliers and technical intermediaries (to what extent the supplier is liable for the Internet user's activities, criminal activities, child pornography, etc.) or the inviolability of postal secrecy.

III.4 PRIVACY ISSUES IN THE INFORMATION SOCIETY

Because privacy is a real concern for end-users of the information society, because cybercrime needs increased justice and police investigations, it affects effective privacy solutions. This section addresses some stakes, challenges, threats and privacy issues. Basic guidelines are identified to preserve privacy and satisfy security objectives for all actors of the information society.

III.4.1 Privacy definition and main issues

Based on Oxford Dictionary definition, the *privacy* is “the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion”. The free and unsupervised use of information and communications technologies means confidentiality and integrity of data and flow, without active or passive listening. In digital environments (digital information, dematerialization of actors, computers and networks operating mode), technologies don’t preserve, in native mode, user’s privacy. To give only one example, an Internet Service Provider (ISP) has the opportunity to check traffic, emails, files, etc. which go through its infrastructure. This affects everyone’s privacy over the Internet, and can put in danger e-business activities. Copy, logging and eavesdropping are easy to realize. Network analysis traffic, actives’ auditing, intrusion of detection systems, firewalls, etc. contribute to optimize network performances and security, but at the same time, they can damage privacy of the users. The availability of system’s management tools (as protocols analyzer, monitoring tools) associated to the exponential use of malware, adware, social network, emphasize the importance of privacy needs over the Internet.

The privacy concept in the cyberspace looks like a luxury. Messages are sent as clear text, so that everyone can read them. There is no built-in way to prevent someone from taking something in another person's name. Therefore it is difficult on the Internet (even impossible in some cases) to prove that a person is telling the truth about his identity or claims. Even more, everyone who has access to the computer can examine data stored. The digital coding of information, dematerialization of actors and remote accesses favor illegal access and copy of data. The majority of data on computers is basically not well protected, unless the owner takes special precautions. Eavesdropping, theft of personal or strategic information, commercial proposition, etc. could give economic advantage to unfair competitors.

As more and more information is stored, processed or transmitted by computers and telecommunication networks, the need to insure that this information will not be altered, corrupted and/or stolen becomes more significant. Any thoughts with respect to the own personal information (i.e. medical records, tax records, etc.) will strengthen the opinion that everybody wants, needs or expects privacy.

In September 2000, Amazon.com, Inc. has declared that its customers’ data are *intangible assets* comparable to others.

Nowadays, data confidentiality and privacy protection, when existing, are achieved in a no transparency way to the end user. *Security is done with obscurity*. Moreover, when a website requires

personal information from an Internet user, it is not evident what will happen to that information. What websites will do with that information is not obvious. Will they share it with other entities? And, how long do they keep it?

Users cannot easily see or understand the role of web cookies[37] and the information gathered by them. Most often, *cookies invade user privacy* in a way or another. Users need to understand what cookies are used for as well as all means regarding their personal information.

To satisfy users concerns, websites try to make their practices more transparent. But many privacy policies are models of legal complexity, while others have so little information, rendering them almost useless. Consequently, website privacy policies do not serve their goal of letting Internet users be informed of the use of their personal information.

Effective **privacy culture** and security solutions will contribute to obtain confidence into information and communication technologies. Nowadays, the needs for privacy and security are not yet well-identified and satisfied for individuals and enterprises. In fact, the majority of them consider that information security is only related to anti-spam and antivirus use or to the use of encryption mechanisms in order to achieve authenticity, confidentiality and integrity services. Privacy needs are more often neglected or is ignored by ordinary Internet users.

"In developing countries, human rights organizations understand the need for privacy but do not have the technology. Those in developed countries have the technology but do not think that they need to protect privacy"[38].

Digital traces are generated by any e-activities. These traces can be stored and handled on a legal basis or not. Justice and police investigation, computer forensic as commercial and marketing purposes or state and government policies, for example, could take advantage of personal data, linked to digital traces, in order to achieve specific objectives.

Technologies such as the Internet, sensors, mobile phones, global positioning systems (GPS), biometrics, smart durst, cameras and microphones, etc., are all around us. Pervasive computing is a reality. As information technologies resources continue to propagate and to be interconnected, it will become possible to gather information about virtually everything and everyone, anywhere and anytime. Consequently, privacy issues are becoming a major concern for information society citizens and organizations.

III.4.2 Privacy stakes and challenges

Nowadays, cyber-criminals, hackers or crackers, what ever we call them, represent a real threat to the society, causing malicious harm to ICT resources, to individuals, organizations and states.

By their capacity to intercept data, to intrude systems and access data, *cyber-criminals are able to affect users' privacy*. Deployment of phishing attacks[39] as well as social engineering[40] techniques contribute to end-user's losses of personal information (addresses, financial information, account

---

37 Web / **Internet cookies** are short programs used by web servers which contribute to identify and to personalize services to end-users.

38 Robert Guerra (Privaterra) - The pan European ministerial conference of the World Summit on the Information Society. Bucharest. Nov.2002.

39 **Phishing attacks** aim to gather confidential information by luring the user with a message, which seams to come from a legitimate organization. Phishing attacks rely on social engineering and technical practices. The main motivation is financial gain. Phishers will either commit fraudulent acts with the collected information or they will sell it online in a public forum.

40 **Social engineering**: Techniques, procedures and measures used by malicious attackers, who usually take advantage of the users' credulity to, *inter alia*, obtain their passwords and connection parameters and usurp their digital identity, in order to trick and breach the system by pretending to be authorized visitors.

information, passwords, etc.). This kind of information represents precious targets for cyber-criminals, offering them the possibility of use for illegal actions.

The digital identity theft has increased in an exponential manner since 1999. This phenomenon cannot be ignored and will continue to amplify, since no action is taken to protect and to dissuade. One of the most utilized methods to carry out such robberies is malevolent software (*malware*) as virus or Trojans. Trojans are a kind of virus that can be hidden inside executable files (like mp3 songs, free games, pictures, movies...). Once the file holding the virus is executed, the Trojan could provide information to the cyber-criminal in a transparent manner. *Most often, the Internet users have no idea that their private information has been stolen*. This information could be used to perpetrate criminal actions. A stolen identity user is responsible of malicious activities that he didn't perform! In this context, he has to prove his innocence, which is difficult, even impossible without any help.

Individual criminals as well as organized crime take advantage of the Internet facilities. Consequently, police investigations in information and communication environments are more and more necessary and frequent. It relies on computer forensic and digital traces analyses that constitute an emerging scientific police specialization. This involves information gathering and flow and data monitoring. These processes must be well mastered and controlled, respecting democratic principles and rights as they raise issues of privacy. They need to be integrated in an appropriated legal framework, which must be enforceable, both at national and international levels.

III.4.3 Needs, constraints, policies and tools

Nowadays, society has to deal with major contradictions present, between justice and police investigation needs and privacy and freedom protection for individuals, corporations, governments and countries' needs.

Many stakes and challenges are related to privacy protection on the Internet. The ***basic rights of privacy must be respected and guaranteed to all users*** wherever they are located. Effective e-privacy solutions should be implemented in information technologies resources in order to provide the minimum level of confidence essential for an effective digital economy. Efficient e-business and e-government activities must integrate information security and privacy solutions.

A trusted information society where democracy is not a virtual concept could be built, if and only if, security and privacy issues are solved and civil and national security needs taken into consideration.

Privacy stakes couldn't be dissociated from information security stakes. Concrete, simple, efficient, flexible, comprehensible measures must be taken.

It is only by taking into account the *need of privacy protection and security* that an enforceable *legal framework* could be defined. At the same time, *tools* should exist and be implemented to contribute to *preserve privacy requirements*. To give only one example, the Electronic Privacy Information Centre (EPIC)[41] offers an Online Guide to Practical Privacy Tools. Many methods are defined and presented in this guide such as steganography, file wiping, anonymous remailers and encryption.

- The *steganography* is a process of hiding information within others. This method is rather used by criminals and for malevolent intendings.
- It is not common use for the end-users. Often files, which a person believes he has deleted, are not really destructed. A *file wiping program* ensures that sensitive material is truly destroyed.
- *Anonymous re-mailers* offer services, which provide a way to send e-mails more or less anonymously. Few users are aware of these techniques.
- The encryption is simply the transformation of data into an apparently random and less readable form through a mathematical process. Encryption is a part of cryptography, which is the science of disguising information. The transformation process (the encryption) usually involves an electronic key, which is a suite of digital bits working like a key to a lock in the

[41] Electronic Privacy Information Centre: http://www.epic.org

real world. The fact of encrypting data is like putting it into a secure logical folder, shutting it with a key. The reverse transformation (decryption) may require the same key (symmetric cryptography) or a different key (asymmetric cryptography) and allows the extraction of the original data.

Some recommendations relate to the form of *privacy policies* published on websites, the others affect directly the contents of these policies.

First of all, the published policy must give at least an answer to the users' needs of understanding privacy concerns. *Simple and clear answers* must obligatorily be given to the following questions:

- Why and how does the company use personal data?
- How the company will protect these data?
- Is the company using cookies and browsers' identifications?
- Is there any third party during the transactions between the company and the Internet user?
- Will the company share or sell any of the collected personal data?
- Is the company storing or using users' IP address?
- Will the company notify their users about any changes of the privacy policy?

Secondly, the user must find all the details in only one website (i.e. no need to consult other websites to have an idea about the policy). Finally, the company has to prove that it will apply all the terms of the policy. This point is directly related to the laws in the different countries.

As the users need to discern technological and informational elements to build the confidence in online services, these points could furnish to Internet users informational and technological elements, necessary for the installing of confidence in E-services and E-business. Without confidence, the relationship between the E-services' providers and clients is not possible.

After fulfilling the contents of the *privacy policy web document*, the enterprise must present it in a readable ergonomic form. The policy document must be clear (with a medium police size and paragraph separators) and easy to be understood by all users (not a complex model full of technical terms). The number of pages differs from a company to another, but mostly a document of 3 or 4 pages can contain all details of the privacy policy. An agenda with a hypertext link at the beginning of the document is recommended. This agenda can help Internet users to navigate within the document and check only the fields that they are looking for. All these points can increase users' confidence in online e-services proposed not only by companies but also by governments and public administrations.

III.4.4 A way to preserve privacy

How can one preserve privacy when users offer and relate personal information about them? *The best way to preserve one’s private life is not to leave too much of personal information on commercial servers or on social networks, virtual communities, discussion forums, chat rooms, etc.* Internet servers never forget *and when users give personal data to services, applications, or servers outside his control, they never know how data can be exploited, by whom and for what purpose. Internet users have to keep in mind that personal data represent valuable assets and they should be protected in consequence.*

PART IV

TECHNICAL APPROACH

Part IV introduces a technical approach to cybersecurity, presents the most relevant principles of computer security, and specifies the domains of application of cybersecurity. To ensure the availability, integrity, confidentiality, and non-repudiation of resources and services in networked environment, relevant security technologies are explained; some e-mail and e-commerce risks issues are discussed and security solutions given.

The importance of technical security measures to decrease the number and impacts of cyberattacks is presented. The need is identified for a complementary technical, procedural and managerial security approach towards the control and prevention of informational risks, and towards improving the efficiency of security solutions.

IV.1 PRINCIPLES OF INFORMATION TECHNOLOGY SECURITY

IV.1.1 ICT security criteria

One approach to information technology security is to describe what is expected of the component elements of the information system architecture. Thus, a central component of information system security is, in fact, the usability of the system:

- **The capability of a system to be utilized.** This depends on the *availability* of hardware and software resources and services. It is a function of good dimensioning, sufficient redundancy of resources, back up, recovery and operations procedures adapted to the requirements.
- **The capability of a system to prevent unauthorized persons and processes from accessing data.** This concerns the preservation of data *confidentiality* and *integrity*. These are ensured by: (i) access control procedures such as identification, authentication and authorization with respect to certain permissions or access rights; and (ii) encryption mechanisms.
- **The capability of a system to allow only authorized persons and processes to perform data modification.** Here, an *integrity* criterion is necessary. This involves access control, error control and coherency checking procedures.
- **The capability of a system to prove that actions and transactions have actually taken place.** This involves traceability, proof, administration, audit and non-repudiation of actions and events.
- **The capability of a system to carry out actions and provide its expected services** under appropriate conditions of usage and performance throughout its life span. This involves continuity, reliability, user friendliness and operational soundness.

These various abilities define the security criteria of a system that can be fulfilled through the implementation of appropriate mechanisms (figure IV.1).

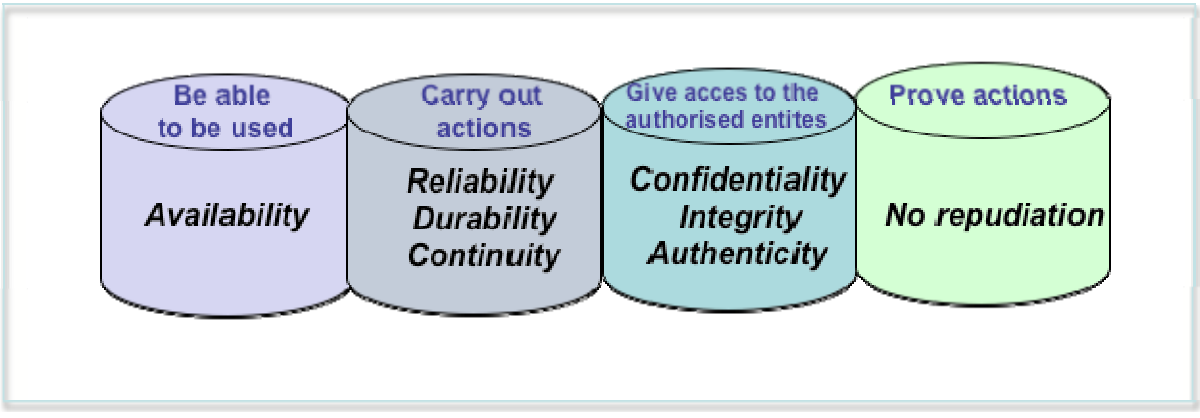

Figure IV.1: Security criteria and system capacity

IV.1.2 ITC Security Domains

Information system security affects all spheres of an organization's ICT activity, and all of its members. Security elements can be classified as follows, according to their area of application (Figure IV.2):

- Physical security;
- Operational security;
- Logical security;
- Application security;
- Telecommunications security.

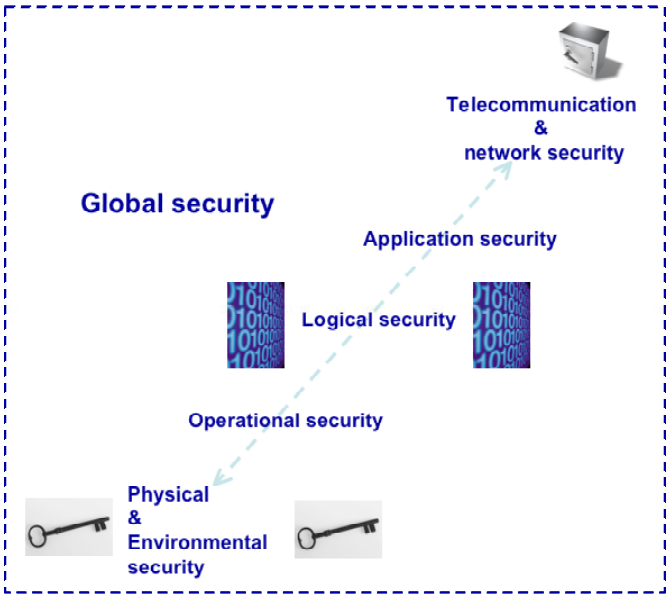

Figure IV.2: Computer Security Domains

Physical security represents the most fundamental and common control for information systems. Sensitive areas are not only ICT and operations areas, but also those that house indispensable logistical equipment, such as air conditioning and the electrical power supply. The three main risks that threaten physical security are (i) physical access; (ii) environment-related dangers (energy supply); and (iii) intentional or not damage caused by natural disaster (fire, hearth crack, …) .

Physical security concerns all aspects relating to systems and environment control. This includes hardware, components, cable, sites, power supply, and air conditioning. Without being exhaustive, the following are basic for physical security:

- Protection of the power supply, the environment and access - physical protection of equipment, distribution centres, connection boards, etc.;
- Traceability of site entry - dissuasion;
- Strict control of keys to access different areas;
- Physical redundancy;
- Equipment labelling - protection by dissuasion;
- Etc.

Operational security refers to everything relating to the proper functioning of the system. This involves the implementation of a set of diagnostic tools and procedures for regular preventive maintenance and repair as well as replacement of defective entity. It includes systems administration

and control, recovery procedures, and relies upon competent staff. The main key points of operational security are:

- Regular, permanent, dynamic (real time) inventories;
- Information technology management;
- Configuration and update administration;
- Monitoring of incidents, and tracking them until solved;
- Operations automation, control and tracing;
- Journals and accounts files analysis;
- Maintenance contract administration;
- Etc.

Logical security primary refers to the management of logical access control, which involves identification, authentication and authorization service (Figure IV.3).

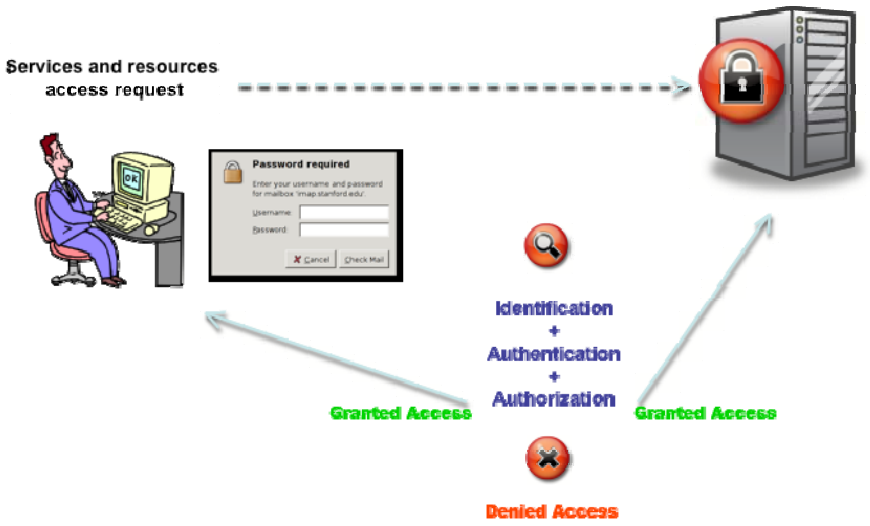

Figure IV.3: Logical Security

Logical security also refers to all *preventive measures* against the infection of data and programs through virus contamination. This includes:

- Protection against malware;
- Efficient management of identification, authentication procedures and remote access;
- Control of the use of portable computers and mobile device;
- Backup and restore procedures (backup of sensitive information onto extractable hard disks stored in secure places, etc.);
- Security control and supervision;
- Systems and networks management.

Logical security mechanisms must be coherent in order to prevent threats, not so much against security tools themselves, but against attacks that might take advantage of logical dysfunction or incompatibility.

It is far easier to assess the monetary value of hardware than of data. Nevertheless, the major part of the ICT environment's added value comes from the *quality* of processed data. The organization's immaterial and human resources constitute its real competitive factors. An organization must understand the role, strategic importance, and link to decision making of information, in order to protect that information. The type of information to be handled determines the level of protection required. It is important to establish a preliminary classification of the data, because that will settle the degree of sensitivity (normal, confidential, etc.). Only then can the organization identify how many and what kind of logical locks to apply. This approach is part of the phase of determining the appropriate *security strategy*. It is one of the key aspects of the organization's *security policy*.

Logical security has to do with the resource access control point-of-view. Application security has to do with the development dimension and the application life cycle of software.

Application security refers to the secure development of appropriate software solutions, and to their harmonious integration and execution in operational environments.

Telecommunication or network security consists of offering to the end user - to the communicating applications - reliable and secure connectivity from *end to end*. Therefore, it must be possible to implement a communication channel between correspondents capable of conveying the data, regardless of the number or nature of intermediary systems or networks. This implies having a *secure network infrastructure*, including access, communications protocols, operating systems and hardware.

Securing the software and hardware resources linked by the networks depends upon judiciously separating or isolating these resources from each other. It is equally important to secure the *application infrastructure* within which the applications are executed on the end systems, at the level of the user's work environment and the applications. This involves time stamping, origin validation, non-repudiation, and confidentiality procedures. Application security should make it possible to ensure the user's *privacy*. Last, *the security administration infrastructure* must be secured, in order to achieve a coherent and efficient secure edifice. Telecommunications security cannot guarantee alone the security of electronic transfer on its own. It is only one required link in the security chain. Networks should not be the weakest link in the information security chain.

Telecommunication security is not very different from computer security. Although networks are vulnerable, they are mere end systems. Malicious acts can also take place in the office at the physical level and not just via transmission lines. Logical security could be ineffective if physical security is underestimate.

Providing a secure communication environment requires securing all the elements in the information technology chain and process. An organization must make a specific risk analysis that approaches telecommunication security as a function of the organization's environmental, human, organizational and information technology infrastructure. For example, it is insufficient to simply implementing encryption mechanisms for data transfer without analyzing other risks in the information system.

IV.1.3 Security Tools

Securing information, services, systems and networks entails ensuring availability, integrity and confidentiality of resources, as well as non-repudiation of certain actions, and the authenticity of events or resources.

Data security is only meaningful if the organization can guarantee that the data and processes themselves are exact. This is the concept of *quality of data and processes*. Assuring the exactness of the data and processes is a prerequisite to ensuring that they will be stable over time. This is the concept of data stability and *service continuity*.

The main security solutions are based upon:

- Encryption or environment isolation techniques;
- Resource redundancy;
- Procedures for surveillance, control and management of incidents;
- Procedures for system maintenance, access control and management.

An organization obtains data security by means of a *succession of barriers* or protection measures that raise the level of difficulty involved in accessing the resources. These barriers do not solve a security problem - they just shift it and transfer responsibility to other entities. In order to obtain genuine security, an organization must *protect and secure the security solutions* themselves. This is the concept of the *recursive nature of security*.

In a global protection strategy, fighting cybercrime effectively involves:

- Increasing the level of effort necessary to perpetrate a crime by effective security technology and management;
- Increasing the level of perceived risks;
- Decreasing the level of expected rewards.

In order to reach these strategic protection goals, information and communication security solutions have to be implemented. For example, it will require more effort for criminals to hack into potential targeted resources if the following measures are put in place: (i) access control; (ii) integrity control; (iii) authentication control; and (iv) monitoring mechanisms. Enforcing network security architecture through the use of firewalls is a technical measure that makes an attack more difficult to effect. In a complementary approach, legislative and regulatory measures help to raise the level of risk perceived by a criminal.

IV.2 ENSURING CONFIDENTIALITY

Confidentiality is the capacity to keep a secret. It consists of the protection of information against unauthorized disclosure.

There are two complementary ways of assuring the confidentiality of data. They are:

- Limiting access via access control procedures;
- Transforming the data in such a way as to render it unintelligible to unauthorized persons via encryption/decryption procedures.

Encryption systems rely on encryption algorithms that modify, with the help of a key, the characters of a given text. They create the appearance of generating random data, thereby producing an encrypted text that is indecipherable without the decryption key. The original text is called a *plaintext*. The encrypted text is called a *ciphertext*. The latter can be safely transmitted over an unsecured network as long as any malevolent person who could intercepted it are not in possession of the decryption key or able to crack the code.

An encryption/decryption key must have a minimum length in order to ensure that it cannot be cracked too easily. If the key is 16 bits long, it can have 65,536 different values that can be easily identified through computer processing. The longer the key, the more different possible transpositions can be built into the code. That means a longer processing time needed to find keys. Code breaking has become relatively simple for keys that are 40 bits long (10^{12} different keys, or in other words, a thousand billion possibilities easily computational). The preference for really sensitive data is to encrypt with longer keys (at least 128 bits) that require a very powerful information technology infrastructure and prohibitive processing times to break them. The best means for criminals to break

an encryption system is for them to procure the key directly from the user or from the system that stores it.

The robustness of an encryption system is determined by the:

- Power of the algorithm;
- Length of the key;
- Capacity of the organization to maintain secrecy regarding security keys.

The algorithm does not necessarily have to be secret. If it is published and thus made public, its robustness can be widely tested.

The more specific a key, and the more its use is limited in time, the more effective the security. It is advisable to change keys very often and to have several keys, rather than just one for the whole information system.

Architectures with two or three levels of keys are common. For those with two levels, there is a base key or master key, from which session keys are derived. For those with three levels, there is a base key for the encryption of session keys in addition to the session keys themselves. The use of a master key, from which others keys can be ciphered, is recommended to obtain a hierarchy of keys. This can restrict the number of decryption elements that can be directly apprehended. Minimizing the risk at the key level implies good key management and a correct understanding of the use of keys.

Confidence in encryption solutions on the market can only be relative, because there are no guaranteed means of verification. Encryption-based security solutions can be compromised through the exploitation of back doors in software, or the duplication and dissemination of secret keys. In addition, there is no guarantee that algorithms currently deemed to be reliable will remain so in the future. These points constitute **inherent limitations of any classical encryption-based security solutions**.

IV.2.1 Symmetric or private key encryption system

To encrypt and decrypt a text, a key must be applied to an algorithm. If the same key is used for both operations, the encryption system is said to be *symmetric*. In that case, the emitter and the receiver have to possess the same secret key in order to communicate confidentially (Figure IV.4).

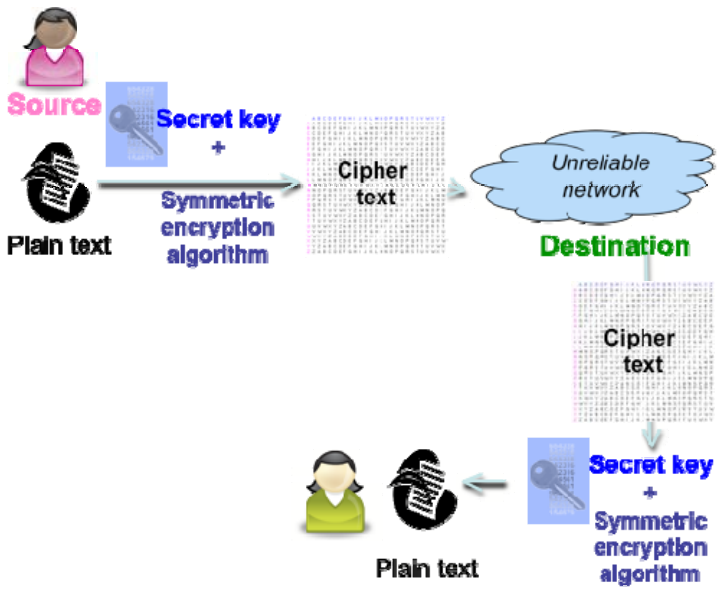

Figure IV.4: Symmetric encryption

A symmetric system requires that the emitter and the receiver agree in advance on the key to be used. Each communication entity manages as many secret keys as interlocutors. Therefore, it is necessary to handle as many pairs of different keys as there are pairs of interlocutors. This process can soon grow to unmanageable proportions. It is badly adapted to Internet, where communication often takes place between entities that do not know each other in a client / server mode where a secret key of a server should be shared among several users. *Symmetric encryption poses serious problems for key management and deployment*. In order to resolve these problems, another type of encryption system, termed as asymmetric or public key cryptography exists and is widely employed over the Internet. The principal symmetric algorithms are AES, 3DES, DES, RC2, RC4, RC5, Blowfish and IDEA[42].

IV.2.2 Asymmetric or public key encryption

A public key encryption system has the capacity to generate, for each interlocutor wishing to communicate confidential data, two complementary keys: *a public key* and *a secret* or *private key*. It is imperative that the private key remains confidential.

Consequently, any sender uses the public key of the communicating partners to cipher data to be sent to them. The sender encrypts the message with the public key of its recipient. On reception, the recipient use his private key to decrypt the message (Figure IV.5).

[42] DES (*Data Encryption Standard*) from NIST (*National Institute for Standards and Technology*, USA) dates from the beginning of the 1970's. A number of different variants, such as Triple DES, DES, DESX, GDES, RDES, are derived from this algorithm. They use longer keys, which makes them more powerful. The Triple DES takes its name from the fact that it has three levels of encryption. The IDEA algorithm (*International Data Encryption Algorithm*) was developed by Ascom Tech AG in Zurich. It is based on a 128-bit key. RC2, RC4 and RC5 developed by RSA Security Inc. They are proprietary algorithms with symmetric keys. They use variable length keys that can be as long as 2048 bits. However, only 128-bit keys are authorized for export from the USA for the RC2 and RC4 algorithms. Blowfish was developed by B. Schneier in 1993. AES (Advanced Encryption Standard) is the successor of DES. It was designed by Rijmen and Daemen in 1998 and approved by the NSA in 2003. AES uses keys of 128, 196, or 256 bits with blocks of 128 bits.

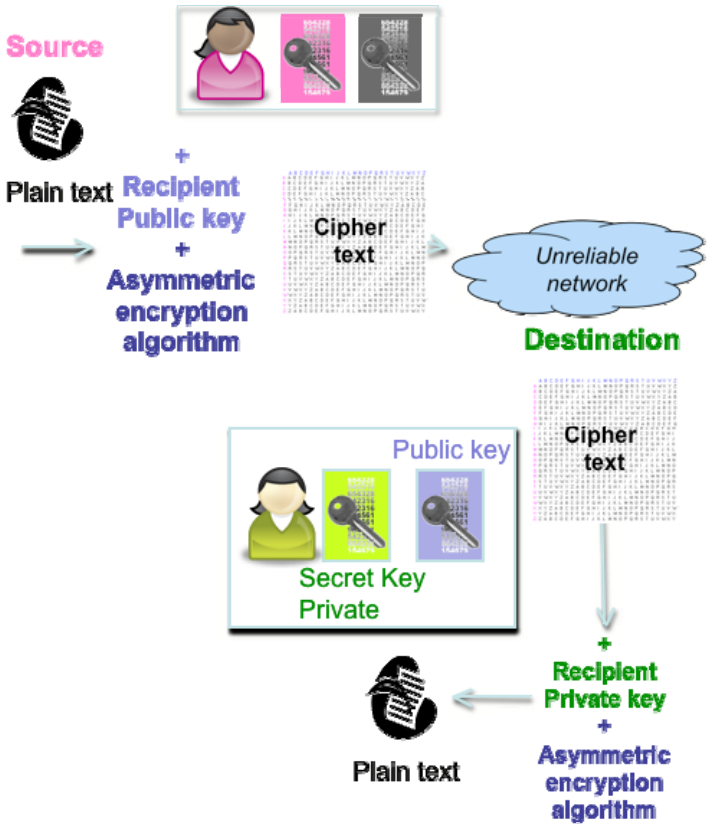

Figure IV.5: Assymetric encryption

The principal public key algorithms, which bear the names of their inventors, such RSA (R.Rivest, A.Shamir, L.Adelman); Diffie – Hellman; El Gamal for example, most often use key lengths varying from 512 to 2048 bits. The execution time of these algorithms produces important overheads that render the encryption of long messages very long and degrade the overall performance of the system. By reducing these processing overheads, new algorithms based on elliptic curve cryptography (ECC) should solve the problem of excessive resource consumption.

IV.2.3 The best of symmetric and asymmetric systems

The major disadvantage of a public key encryption system is that it takes too much time to process long messages. Encryption experts have combined the best aspects of symmetric and asymmetric systems, in order to: (i) reduce the amount of information to be encoded in a public key system; and (ii) resolve the problem of secret key management and distribution.

When encrypting long messages, the sender uses a session key that is valid for both interlocutors for the duration of the exchange and is destroyed at the end of the work session. The sender uses a public key asymmetric algorithm to encrypt the session key, and uses a secret key symmetric algorithm to encrypt the message itself.

The dialogue process would unfold as follows:

1. One of the partners of a communication generates, by a random process, a secret key called a session key;
2. The message is encrypted with this *session key* and a symmetric key algorithm;

3. The session key is then encrypted with the public key of the recipient, which constitutes the digital envelope of the message;
4. The sender sends the encrypted message and its envelope to the recipient;
5. The recipient decrypts the envelope with his private key in order to discover the session key that he will use to decrypt the message;
6. The recipient can use the same session key to send an encrypted message to the sender.

IV.2.4 Key management

Like other sensitive data, secret keys need to be protected and memorized in a confidential and reliable manner. The security of the encryption process, also known as "*sealing process*", relies largely on the security and confidentiality of the keys used.

The roles of a key management system are as follows:

- Generation of a single key; random choice as a function of the algorithm;
- Key distribution, following mutual authentication by interlocutors;
- Key distribution management - limiting access to keys to authorized users only;
- Ensuring secure storage through encryption of keys and reliable archiving for control reasons; search for inactive keys that could be used later, evidence in case of disputes;
- Trace function, error logging;
- Destruction of useless keys;
- Support for intrinsic security functions, such as operational test functions malfunction alarm and recording, key invalidation and key access control (key confidentiality and integrity).

The functions of a key management system reflect the different phases of the key's life cycle These phases are: (i) creation; (ii) storage; (iii) distribution; (iv) use; and (v) destruction.

The life cycle of an encryption/decryption key depends on its use. It is always a good idea to periodically change the value of the keys. It may lead to complexity if the key is modified too frequently. Nevertheless, for all networked applications, it is advisable to change the key for each new work session or even to use more than one key during a single session. There are several systems with single keys, such as those used with smart cards.

IV.2.5 Public-key infrastructure (PKI)

A public-key infrastructure (PKI) is a system that can support public-key encryption, digital signature services and certificate management. It authenticates users based on the user's presentation of a digital certificate. It generally involves multiple certification authorities cooperating to satisfy worldwide Internet communities.

It is impossible to memorize the public keys of all potential correspondents or request them before each issuance. However, as it is imperative to obtain these keys if an asymmetric key encryption system is to be used, one must be able to rely on the services of a third party entity. This is called a **certification authority**. It offers the following services: (Figure IV.6):

- Generation of one "private key – public key" pair and assignment to an entity or person;
- Memorization of the information required for the management of the pair of keys;
- Distribution of the public key to the entities that request it and are authorized to obtain it (this involves the concept of filtering);
- Certification of public keys.

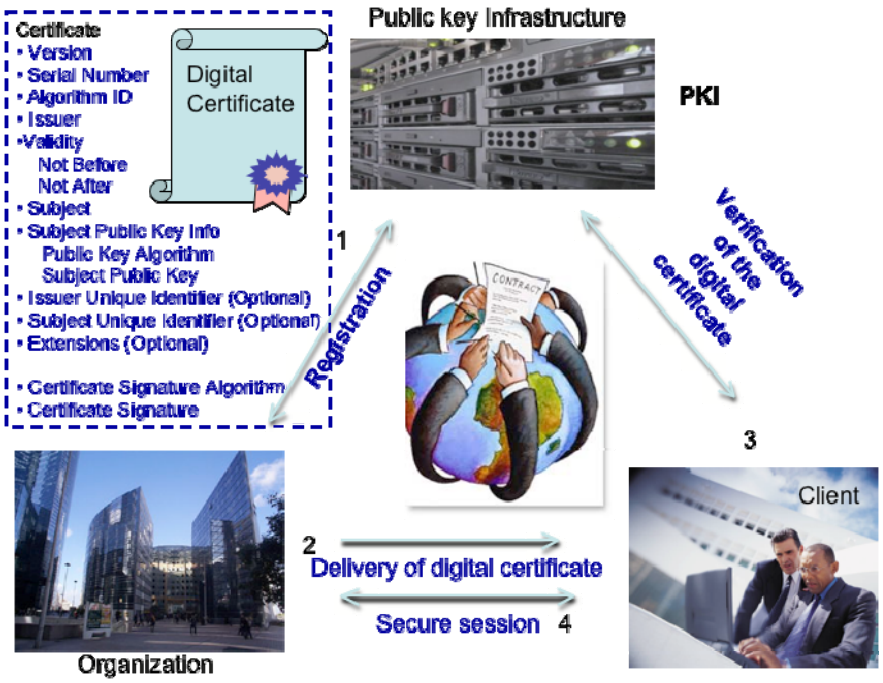

Figure IV.6: Public key infrastructure

Client certificates are assigned by certification authorities who issue digital certificates.

A certification authority has the following tools:

- A web server that processes certification requests made by clients;
- A highly secure administrative server for the management of requests and signatures of certificates. Its roles are: (i) to notify clients by mail or e-mail of the URL (Unified Resource Locator) where the signed certificate can be found; (ii) to manage the certificates revocation list; and (iii) to renew certificates;
- A database that records various certificates, including public certificates from the certification authority, server certificates, directories, personal addresses, and electronic addresses.

Certification is the procedure used to validate an entity's identity. It is the means used to confirm that a given public key actually belongs to a particular entity. *Digital certificates* can be used to ensure both communicating partners that the entity on the other end is authentic.

A certificate can be viewed as an entity's electronic passport. It bears the entity's name and a public key. It contains the expiration date, and the identification and the signature of the certificate's issuer. It also contains various kinds of information of an administrative or general nature.

IV.2.6 Ensuring proof of origin by digital signature

For authentication purpose, a sender creates a message and attaches a digital signature to it, in order to reassure the recipient that the source of the message is genuine. This contributes to the authentication of the sender and guarantees non-repudiation of an emission (proof of origin). A **digital signature** is based on the converse use of the public key encryption algorithms, according to the following basic principle (Figure IV.7):

- A sender creates a small message declaring identity – for example, "My name is James".

- The sender encrypts the message using his private key, in order to constitute an encrypted signature that is attached to the message to be sent.
- The sender then uses the public key of the addressee to encrypt the message and the signature. He then sends the message.
- After receiving the message, the addressee decrypts it with his private key. He then detaches the signature and decrypts it with the public key of the sender.

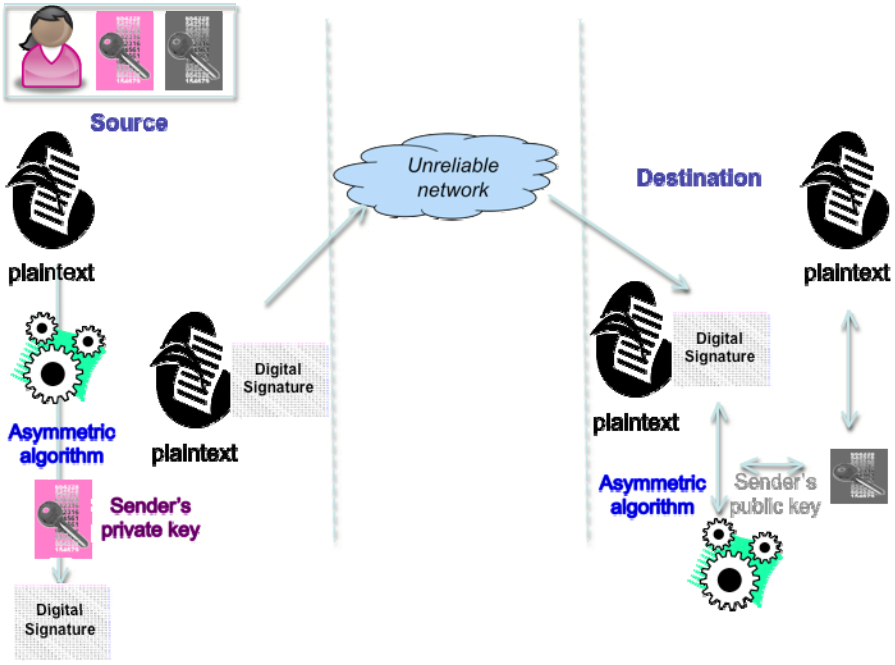

Figure IV.7: Digital signature

Usually, the short message is simply a summary of the entire message. The sender produces it by the use of the hash function[43].

The electronic signature system does have weaknesses. There is nothing to stop someone from cutting out the digital signature from a previous message and reusing it in replacement of the real sender. It is also possible to create a partner's digital signature after having stolen the latter's private key.

A more secure variant of this signature mechanism would be to randomly generate the declaration of identity. This would be sent to the addressee, who would sign it with his private key and resend it to the sender. Any algorithm could be used for this. In 1994, the NIST and the National Security Agency of the USA developed an algorithm called DSA (*Digital Signature Algorithm*) to be used with the DSS (*Digital Signature Standard*) on the basis of the El Gamal algorithm. The scientific and economic sectors have been reluctant to adopt this standard because of its governmental origin.

IV.2.7 Ensuring resources integrity

To be sure of data integrity consist be able to verify that information has not been modified during computation, storage or transmission.

The integrity of the data must be guaranteed by protection against interception and modification. That can be accomplished by utilizing complementary security mechanisms such as the following:

[43] See the following paragraph related to integrity check.

- Rigorous access control;
- Data encryption;
- Malware protection.

Ensuring integrity through **digital fingerprinting** is possible by a specific use of encryption mechanisms. An integrity checking service is assured by utilizing a *summary*, which is created by applying a calculation function to the data content, with the data. If the summary is recalculated and a different result obtained, this will prove that the content has been modified. The summary itself may be encrypted before data is transmitted or stored.

Symmetric or asymmetric key encryption systems make it possible to determine whether the data has been modified. This contributes to ensuring integrity control, but it will not detect if the data has been completely destroyed.

In order to have quality integrity control, a function is applied to the original message transforming it into a small group of bits that constitute a sort of **digital fingerprint** (Figure IV.8).

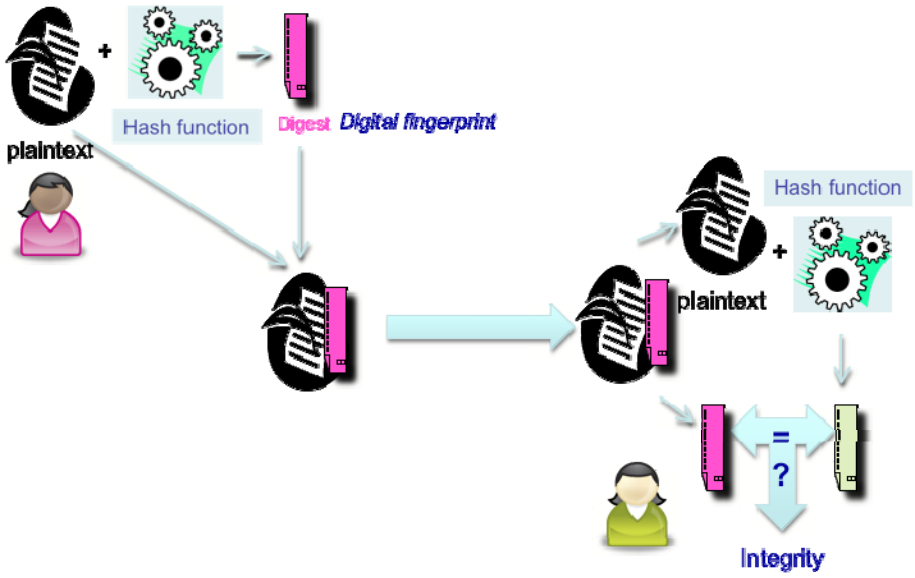

Figure IV.8: Digital fingerprint

A function, known as the *digest function*[44] or *one-way hash function*[45], generates a **message digest**. The latter is a digital fingerprint that is shorter than the original message and incomprehensible. The recipient deciphers the message and its fingerprint with the public key of the sender. He then recalculates the digital fingerprint, using the same hash function on the received message, and compares it to the one that was transmitted. If the result is identical, the receiver has verified the identity of the sender and ensured the integrity of the message. If the message is altered, even only slightly, the digital fingerprint will be considerably modified.

The concurrent use of encryption techniques, signatures and digital fingerprinting makes the stamping of messages possible and guarantees data integrity and authentication. These procedures consume processing time and slow down performance in the operational environment considerably, even if a

44 There is a large number of digest functions. The most common are MD4, MD5, from Ronald Rivest, which produce a 128- bit digital fingerprint, and SHA-1 (Secure Hash Algorithm) from NIST, which generates a fingerprint of 160 bits.

45 The transformation is only made in one direction. Deciphering and same number generation are not possible using two different messages.

broadband network and powerful systems support that environment. Therefore, it is essential to apply these techniques only when strictly necessary, after carrying out a preliminary analysis of what should be protected from which risk. By determining the degree of sensitivity of the data and the security objectives, an organization limits encryption strictly to pertinent data and the applications and transactions concerned.

Ensuring integrity through protection against malware. The consequences of malware program execution can lead to partial or total data or program destruction and to denial of service. Beyond the technological impact, the infection of an information system is always dramatic. It can even be fatal for an enterprise.

Malware protection is a permanent concern for the administrator of the information technology park. It contributes to data and program integrity and ensures service availability, accessibility and continuity. The following measures for example strengthen the protection of ICT resources from malware infection:

- Application of strict directives concerning the use of software other than that distributed, authorized and licensed by the enterprise (authorized software only);
- Restriction of the loading of remote programs;
- Filtering of imported data;
- Rigorous control of software configurations;
- Provision of appropriate information to the users (network use policy);
- Safeguarding of data and programs after verifying the harmlessness of their content;
- Checking of emails and their attached files when transiting via mail servers;
- Etc.

Generally, computer security is limited to viral protection. Figure IV.9 illustrates three phases of the fight against viruses. Those phases are: (i) control; (ii) prevention; and (iii) reaction.

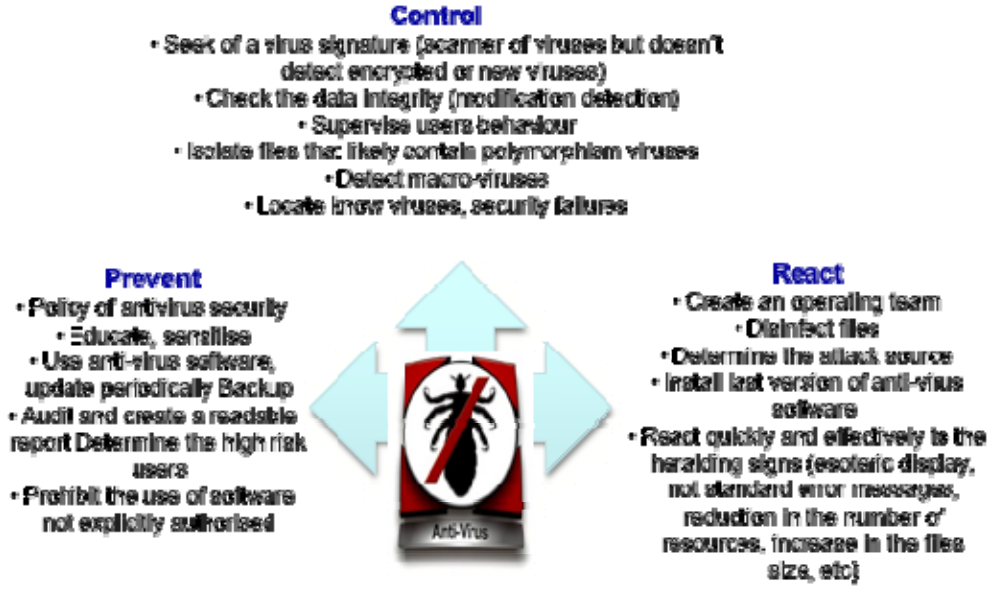

Figure IV.9: Fighting against viruses

IV.2.8 Ensuring resource availability

The availability of services, systems and data is realized through the correct sizing and redundancy of the constituent elements of the information system. A company must be able to assure a nominal service with a minimum amount of interruption. This is the concept of **service and business continuity**.

Backup procedures are indispensable. They must be automatic and integrated with the work of the user. Numerous tools are available for the periodic and automatic backup of all or part of the data on a station or a server. It is also essential to to develop and publish data restoration procedures, so that users know what to do if they have a problem of data loss. The administrator should define a clear backup policy and strike a balance between the cost of backup and the risk run. A data backup policy answers such questions as: What is to be backed up? When? Where? How? If an organization does not manage backup and data storage correctly, data loss is possible.

The network manager is responsible for the creation of user accounts. Each account is given a username (or login name). The username is unique and serves to identify the user when he enters his personal network connection password. The administrator attributes or imposes rights or restrictions on each user. This enables the administrator:

- To limit the number of concurrent user connections;
- To restrict the period for the use of network resources;
- To fix the maximum length of passwords;
- To require the periodic modification of passwords and the verification of new passwords;
- To prohibit a user connections on a certain machines;
- To attribute rights on directories or files on the server;
- Etc.

Apart from the creation and destruction of user identification, the network manager should only intervene, in principle, to modify password that has been forgotten. *It is not because a system administrator has the opportunity to spy, to intercept, to look at any transaction or content that he/her has to do it!*

IV.2.9 Ensuring a non-repudiation service

A **non-repudiation service** provides protection against rejection or denial: (i) that a message has been sent or received; or (ii) that an action or transaction has taken place. For example, it makes it possible to prove that a person is linked to a given event or action.

Non-repudiation is based on having a *signature* or some identification / authentication that proves the identity of the person who created the message. In order to provide this service, a public key encryption algorithm is required. A trusted third party or certification authority may assume the role of notary. The third party officially informs and registers all actions and transactions between the parties, in order to certify the veracity of the exchanges. For this to be effective, the partners must subscribe to this service with a recognized organization that is safe and reliable. The trusted third party is a sort of referee that registers operations carried out between the different parties.

A **cyber notary** is a new type of intermediary. The demand for cyber notaries is growing in proportion to the expansion of commercial and financial transactions on telecommunications networks. This role of veracity guarantee could be extrapolated to all sorts of electronic applications that operate in cyberspace.

Log procedures and tools help to register many kinds of relevant information that could be exploited for audit procedures, to trace events or activities, identify the origin, circumstances of incidents, etc. for example. Logs' information should be analyzed on a regular basis to learn about operational mode and behavior of systems and users in order to be able to improve security effectiveness and efficiency.

An incident that occurs at a first time is an error; the same repetitive incident constitutes a fault! It is not enough to store data if they cannot be retrieve or exploited when required. Moreover, sensible logged information has to be protected against illicit modifications.

IV.3 IMPLEMENTING SECURITY WHILE ACCESSING RESOURCES

IV.3.1 Conventional access control

A **logical access control mechanism** serves to limit access to information resources. It is based on the identification and authentication of individuals, and on the permissions or access rights that have been granted to them (Figure IV.10).

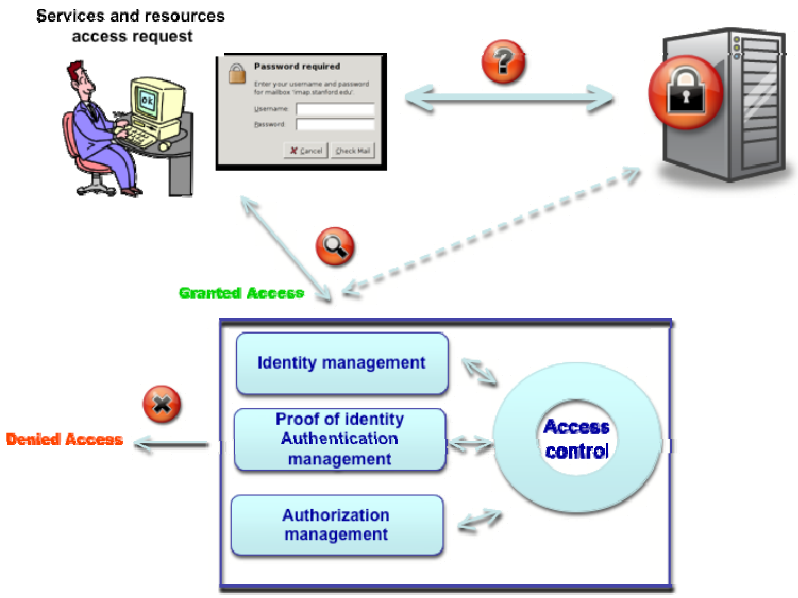

Figure IV.10: Basic components of logical control

One of the cornerstones of **access control** is the identification and authentication of information system actors. Authentication makes it possible to confirm or contest users' identities.

The purpose of the **authentication** service is to ensure that the stated identity is authentic. This is the concept of **proof of identity**. One or more of the following factors generally determines authentication:

- A secret that is known to the entity in question, i.e. a password or *Personal Identification Number* (PIN);
- An item in the entity's possession, such as a card for example;
- A feature unique to the entity, a physical attribute such as a characteristic trait (fingerprint, voiceprint, or retina print).

The process of identity verification works as follows: The individual requesting access states his identity and provides an item of proof that he alone is supposed to know or possess. This could be

a password, confidential key, or fingerprint. The authentication service then compares that information with the data stored in its authentication server.

Mutual authentication refers to authentication of both the user and the server / service requested by the user.

An authentication server must be extremely well protected. It must be secured by ad hoc mechanisms providing access control and secure systems management. The data it contains must be encrypted. An authentication server must not be vulnerable or subject to faults, because the overall security of the information and telecommunication infrastructure depends on its robustness.

The control access system grants or denies access to on the basis of the identification-authentication process and on the fact that access rights and permissions[46] exist and that they are managed correctly.

On the basis of an authenticated identification, the access control mechanism allows access, according to the user's profile, to the requested resources. This presupposes that the **identity management**, *identity proof management* and *authorization management* have been properly effected vis-à-vis the user.

The *user profile* contains all of the data on which access authorization decisions are based. It must be carefully devised in accordance with the access management policy. The purpose of authentication is to associate the notion of identity with a given individual. Access authorization entails selective filtering of requests for access to the resources and services provided by the network. The system utilizes a triple control that covers usage rights, coherence with the service requested and the characteristics of the access device. Then, a three dimensional indicator is used. It contains the following profiles:

- The user: access rights as a subscribing customer;
- The equipment (device): hardware and software description;
- The service: network and hardware requirements.

Control of access rights consists of verifying whether the service in question is registered in the user profile.

IV.3.2 Access control based on biometry

Biometric individualization consists of using biometric data for checking the identity of individuals at the point of access to premises or within the framework of judicial supervision (by the police, etc.). This includes the following types of data: fingerprint, voiceprint, face, ear, hand geometry, retina, and iris. Biometric individualization makes it possible to do away with passwords, replacing them with physical characteristics from which a binary data value can easily be extracted.

The first step is to extract and record the given individual’s *biometric characteristics* in the form of a "biometric template". Such recordings must be highly reliable and securely stored (Figure IV.11).

[46] Permission, as a function of certain access rights, is most often expressed in terms of read; write, creation, destruction and execution rights on logical resources.

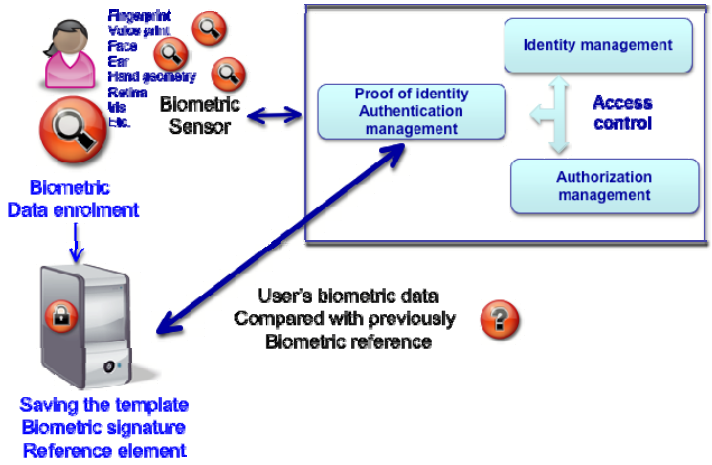

Figure IV.11: Biometric access control

The authentication process may be lengthy, since the comparison phase has to account for the variations inherent in the live nature of the compared data. For example, voice samples will never be completely identical. The comparison is based on *statistical* and *probabilistic* processing of the biometric data. This method is not **foolproof**. It is impossible to determine with 100 percent certainty that the person screened is who he claims to be. The *error rate* of these systems is still high – utilized alone, they cannot provide a high level of security. Nevertheless, when combined with "conventional" authentication mechanisms based on passwords, the biometric side serves to enhance the level of security provided. This combining of two different types of authentication mechanisms is called *dual verification.*

The expanding use of biometric technology *raises numerous issues* of an ethical and ergonomic, not to mention economic, legal and technological, nature. These issues include:

- The confidentiality of biometric data that may be considered private;
- Cases in which biometric data may not be unique (identical twins);
- The fact that biometric data sensors are often seen as intrusive and are rejected by the majority of users in cases where a choice is available. They also constitute a threat to the freedom of the individual, e.g. a large number of sensors, such as video cameras, set up in public locations and operating without people's knowledge;
- Cases of identity theft or of improper or fraudulent use of biometric data.

Given their lack of precision and continuing high purchase, deployment and operational costs, access control solutions based on the use of biometric data are not in mainstream use.

Summary of the limitations encountered when using biometric data for access control:

1- Biometric data used in the identification of an individual will vary through time.

2- Biometric data have to be captured and converted into a reference sample for storage in a database. As they are digitized, the data become fragile (and hence modifiable), and must be accorded the best possible protection. For each access request, the user's biometric data must be captured; this raises the problem of consent in regard to the capture method, and the associated feeling of intrusion.

3- Access control based on biometric data is not 100 percent failsafe owing to the variability of the human sample to be analyzed. Depending on the system used, the probability of false positive or false negative identification can be relatively high. In

addition, the reliability of the result will depend on the technology used to record the biometric data, and the overall quality of the operation.

IV.3.3 Access control based on digital certificate

The use of passwords for the authentication of users of a web server is fairly simple. Nevertheless, there is a risk that it could be ineffective, because it is difficult to manage an efficient password system for a very large user population. The large number of servers and users could render such a method unworkable, since too many users would know the server password.

A security mechanism based on certificates helps to resolve this problem and presents two advantages. First, it allows for a large number of users, and second, it makes it possible to have distribution of a decentralized verification system. Therefore, the use of certificates makes it possible to implement a control mechanism that is relatively selective.

A certificate contains its owner's public key and name, the name of the certification authority, a serial number, and various additional attributes. The latter might include digital or textual information, such as a postal or electronic address, employer, job position, division/department, office number, telephone number, date of birth, sex, or nationality. These attributes provide the site administrator with flexibility in controlling and restricting access as a function of the value of one or a combination of attributes.

A browser must present a certificate and *proof of ownership* in order to contact a server that uses a certificate-based security mechanism. If the authentication is positive, the server then checks the user's rights to the requested resources, either directly on the basis of information contained in the certificate, or by consulting a database. In the latter case, the certificate is only used to identify clients, and access rights are stored in an external database. While this approach makes it possible to separate user identity from user privileges, it poses problems for the design, update, access and performance of the database. On the other hand, if user rights are associated with user identity independently of a database, a server can accept certificates coming from various certification authorities. However, that method poses the following problems: (i) the system is dependent on the life cycle of the certificate; and (ii) the system is vulnerable to problems relating to information updates on the certificate, its pertinence and its validity. Furthermore, the server must be able to manage a certificate revocation list, which involves accessing an external database, thereby cancelling out the advantages of this solution.

Certification can be an efficient means of carrying out access control, but it is not the ideal solution. Its limitations involve the following:

- Establishing the veracity of the certificates;
- Establishing confidence in the reliability of the certificates;
- Implementing an efficient and reliable way to attribute and manage the certificates. It is fairly easy to allocate a certificate to a user. It is far more difficult to revoke it.

An effective method for revoking a certificate is essential in the following circumstances:

- The information contained in the certificate becomes obsolete;
- The user's private key has been compromised;
- The user has lost the password needed to unlock it;
- The user has left the enterprise. After a certificate has been revoked, the server inscribes it into a **Certificate Revocation List (CRL)**.

It is for the certification authority to administrate revocation lists containing the numbers of all invalid certificates, and to consult them at every request. The overhead of a systematic consultation of this database decreases the performance of certification-based access control systems. At present, one "practical" way of cancelling a client's certificate is to wait until the expiration date. It is essential that certificates are designed in the light of this constraint and the internal risks posed by employees.

The following are other problems associated with certification:

- Users sometimes forget or divulge their private key deciphering passwords;
- Sometimes a certificate or a private key becomes altered. Incidents may then occur on the user's workstation or during the update of the user's browser. Therefore, ways and means must be provided for the recovery of the private key.

The benefit of a certificate-based access control mechanism resides in the fact that only the certificate owner knows the private key corresponding to the public key contained in the certificate. However, it is possible for criminals to forge digital signatures by guessing the private key or the encryption algorithm.

Therefore, the confidence in the certificate depends first on the robustness of the encryption algorithm employed, and second on the level of security applied to the user's private key. The latter is generally archived in encrypted form on the PC and unlocked each time the browser needs it.

The *degree of reliability of the certificate* depends on the capacity of the certification authority to verify the veracity of the identification of a user requesting a certificate. The procedures for requester authentication vary from one authority to the next. It is the certification authority's responsibility to be able to effectively track the requester's identity.

The overall security of the system depends on the security of the private key of the certification authority. Indeed, if this were to be stolen, the thief could issue certificates and pretend to be the real certification authority.

IV.4 IMPLEMENTING SECURITY DURING DATA TRANSFER

IV.4.1 Routing procedures and security

Switching and *routing* functions are complementary and address two types of issues:

- Optimization of the sharing of network resources;
- Routing of data from a sender to one or several receivers.

Servers use switches for the routing function and for interconnecting transmission lines. The physical connection inside the switches depends on their internal architecture. Several different switching techniques exist. The choice of switching technique is dependent on the resource sharing mode, the level of communication desired, and the privileged criteria for service quality.

The routing function determines the best route for data to take between source and destination. Switches that are called "routers" often support this function.

- The routing function is determined by:
- The routing policy;
- The routing tables;
- The routing algorithms;
- The network administration.

The *routing policy* is a transport strategy choice that reflects the way in which the network administrator manages the operation mode of the network. It depends, among other things, on the ability of routers to support these administration choices. Static policies, where routers are predefined permanently regardless of the state of the network, are distinct from dynamic or adaptive policies. The latter enable adjustments to be made to information in the routing tables. This allows routers to take a routing decision based on network characteristics, current traffic, and the state of the lines and systems (availability, performance, loading).

Ideally, a router should be able to accept all packets. This means that the adjacent router does not convey data to it if the data cannot be processed. The best route is not necessarily the shortest. The best route is one that passes through lines and routers that are capable of handling the traffic. A router should not lose or corrupt data, or mobilize it for too long. It needs to have sufficient memory and an efficient queue management system.

Performance, quality of service, availability and reliability of the network largely depend on the intelligence of routers and their ability to adapt to routing decisions and context.

A router can carry out switching of incoming packets on outgoing lines towards the next switch/router, using addresses contained in its routing table. The routing software utilizes a routing table that is designed according to a specific algorithm.

Routing table modification must be done in a secure way. Only authorized and authenticated entities should be able to access the contents. Otherwise, there is a risk of denial of service, illegal address modification, packet redirection, packet hijacking, packet destruction, etc.

IV.4.2 Name server and security

A **name server** or **DNS (Domain Name Server)** provides a directory service and mainly supports the correspondence between an entity's logical name (URL or email address) known by users or applications and its IP address (known by routers). Users or software applications only know the name of a requested entity, and not its IP address, so any communication relies upon name servers. They can also carry information relating to user or resources identification, permission, access rights and localization. *Name servers security* mechanisms are mandatory to prevent several types of attacks as packet redirection, packet hijacking, intrusion or denial of service for example. Those mechanisms include consistency checks, duplication, authentication, access control, encryption, and events logging.

IV.4.3 Secure IP Protocol (IPv6 & IPSec)

The need to accommodate security requirements led to a revision of version 4 of the Internet protocol. There was also a need to provide for a wider range of addresses, increase the number of available Internet addresses, and allow dynamic allocation of bandwidth to support multimedia applications. As a result, a revised version of the IP protocol was produced called "Internet protocol next generation" (IPnG), or **IP version 6** (*IPv6*)[47].

In 1994[48], the *Internet Activity Board* (IAB)[49] addressed the security requirements of the IP protocol. Version 6 of the IP protocol (IPv6), which was specified in 1995, includes authentication and confidentiality facilities.

The main developments in IPv6 in relation to IPv4 relate to the following points [RFC 2460]:

- Expanded address space and address hierarchy: address size increased to 128 bits (16 octets) from 32 bits (4 octets); addresses represented in hexadecimal numbers[50] separated by colons every two octets (e.g. 0123:4567:89ab:cdef:0123:4567:89ab:cdef), instead of dot−decimal notation;
- The possibility of dynamic bandwidth allocation to support multimedia applications;
- The capability to create virtual IP networks;
- The use of options headers to support authentication and encryption procedures;
- The simplification of packet headers to facilitate and speed up routing.

---

[47] RFC 2460 – www.ietf.org/rfc/rfc2460.txt.

[48] RFC 1636: Report of IAB Workshop on Security in the Internet Architecture, 8-10 February 1994.

[49] www.iab.org/

[50] Alphabet of hexadecimal numbering system (base 16): 0 1 2 3 4 5 6 7 8 9 A B C D E F.

Adopting IPv6 calls, *inter alia*, for the modification of the addressing and address management mechanism[51]. It also calls for the installation throughout the Internet environment of systems supporting IPv6, systems operating with both IPv4 and IPv6, and large-scale synchronization of version migration.

For all of these reasons, version 6 has not yet been widely installed, and no government incentive or international recommendation seems to be able to impose adoption of version 6 of the protocol throughout the network. Only mostly private infrastructures incorporate IPv6.

Implementation of IPv6 with its built−in security functions is uncommon. Therefore, to meet network security requirements, an intermediate solution called **IPSec**[52], has been developed and adopted by the Internet community. IPSec is compatible with both IPv6 and IPv4. The Internet Engineering Task Force (IETF)[53] issued several documents in 1995 (RFC 1825 to 1829) specifying ways of securing an Internet infrastructure.

IPSec Protocol offers data confidentiality and authentication services at IP transfer level through an Authentication Header (AH) or an Encapsulating Security Payload header (ESP).

Each application, irrespective of the type of traffic it generates, can use these security services without any adaptation. IPSec operates in *point-to-point mode*: the data are secured between a sender and a receiver via a secure relationship (security association).

The authentication header provides IP packet authentication and integrity services. This guarantees that the data have not been altered during transmission, and that the source address is the one that appears on the packet.

The encapsulating security payload header allows the implementation of encryption mechanisms (symmetric encryption such as DES, Triple DES, RC5 or IDEA), and offers similar authentication services to those provided by the authentication header.

The encryption algorithms use keys that have to be generated and disseminated. Therefore, encryption key management is an important component of implementing IPSec−based solutions. Some of the key exchange protocols are: (i) Oakley key determination protocol[54], based on the Diffie−Hellman key exchange algorithm [RFC 2412]; (ii) Internet Security Association and Key Management Protocol (ISAKMP) [RFC 2408]; and (iii) Internet Key Exchange (IKE) [RFC 2409].

IV.4.4 Virtual Private Networks

The installation of IPSec protocol at access points to the Internet network makes it possible to establish a communication channel (*IPSec tunnel*) between those points whose ends are authenticated (Figure IV.12).

[51] RFC 1886 identified in 1995 the modifications to be made in DNSs to support IPv6.

[52] RFC 2401 – www.ietf.org/rfc/rfc2401.txt

[53] www.ietf.org

[54] Oakley key determination protocol: RFC 2412 – www.ietf.org/rfc/rfc2412.txt.

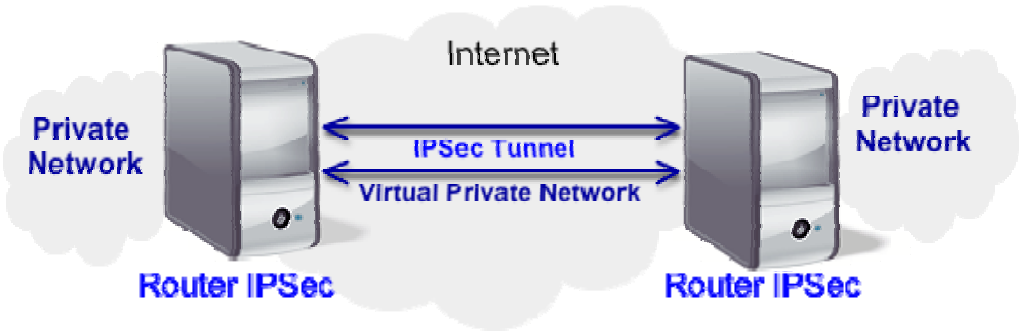

Figure IV.12: Establishment of a VPN using an IPSec communication channel

These ends are located in the organization's systems. This usually ensures that they are physically protected. Moreover, data carried over the connection may be encrypted, according to the option adopted. In that way, a secure route can be set up between two points of an unreliable infrastructure. This is the concept of *virtual private network*. The term "network" is something of a misnomer, since only a (virtual) logical connection is established.

IV.4.5 Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure HTTP (S-HTTP)

Secure sockets layer (SSL) is software that allows a certain level of security to application exchanges. Most web browsers on the market support it. The two communicating parties in an SSL connection are authenticated through a *certification* procedure and a trusted third party (PKI - *Public Key Infrastructure*). They then negotiate the level of security to be applied to the data transfer. The transmitted data are encrypted for the SSL communication. The SSL software is now widely used, notably for the purpose of commercial transactions over the Internet. The third release of SSL (SSLv3) has been adopted by IETF (Internet Engineering Task Force) to give way to **TLS (*Transport layer Security*)**, considered as a new upgraded version of SSL, based on the same principle.

The installation of SSL / TLS has a significant impact from the point of view of the server. It requires certification, which necessitates a dialogue with a recognized *certificate authority* and necessitates firewall application relays that support SSL operation. Certification is sometimes considered to be an impediment holding back the deployment of this solution.

A different solution exists, called Extension to the HTTP protocol **(secure HTTP,** or **S-HTTP)**. It offers the same security facilities as SSL, with the same certification constraints, but only supports HTTP data flows. This solution has not been widely adopted. Most application protocols have a secure version, which generally allows authentication of correspondents and encryption of transmitted data. An alternative to installing new secure versions of application protocols is to establish a common security mechanism offering generic security services for all applications.

The extensive use of *hypertext documents* and the downloading of content, whether active or passive, pose numerous security problems relating, *inter alia*, to: source, author, authenticity, harmfulness, etc. Some responses to this new dimension of information system security are beginning to emerge. These include: (i) techniques for signature of XML documents; (ii) watermarking; and (iii) management of electronic rights. It has to be possible to maintain a given level of security, even if the object to be secured falls outside the physical borders of the environment in which its security is usually managed.

IV.4.6 Intrusion Detection

Intrusions, incidents and anomalies must be detected and identified as soon as possible after they occur and be rigorously dealt with so as to ensure that the systems in question continue to function normally and remain protected.

An incident is an event that occurs unexpectedly. While incidents are, for the most part, not serious in and of themselves, they can nevertheless have severe consequences. An **anomaly** is an exceptional occurrence that can result in abnormal functioning of the information system and a breach of the security policy in force. Its causes may be accidental (for example, a configuration error) or deliberate (a targeted attack on the information system). A given intrusion may be considered as an incident or an anomaly.

Intrusion detection refers to the set of practices and mechanisms used : (i) to detect errors that may lead to breaches of the security policy; and (ii) to diagnose intrusions and attacks (this includes anomaly and misuse detection).

An **intrusion detection system (IDS)** is comprised of functional blocks as data gathering, data analysis, and intrusion detection and response.

IV.4.7 Data filtering and environments partitioning

The separation and masking of a private environment vis-à-vis the public Internet is achieved through the installation of one or more **firewall systems**.

A firewall is a system for filtering or blocking data flows. It analyzes the flow. Then it either authorizes or rejects the flow. *Partitioning a network* can create separate IP environments. This means that the access points of the networks are physically independent of one another. It is an architectural network measure that allows controlling a *network perimeter* and the interconnection of two networks that have different security levels (Figure IV.13). Some particular systems can be isolated in a *demilitarized zone* – DMZ, from others parts of a private network, by using firewall that filter and control the traffic requesting an access to them or the traffic generated by them. The installation and configuration of a firewall are based on the network architecture selected to meet the security and control requirements.

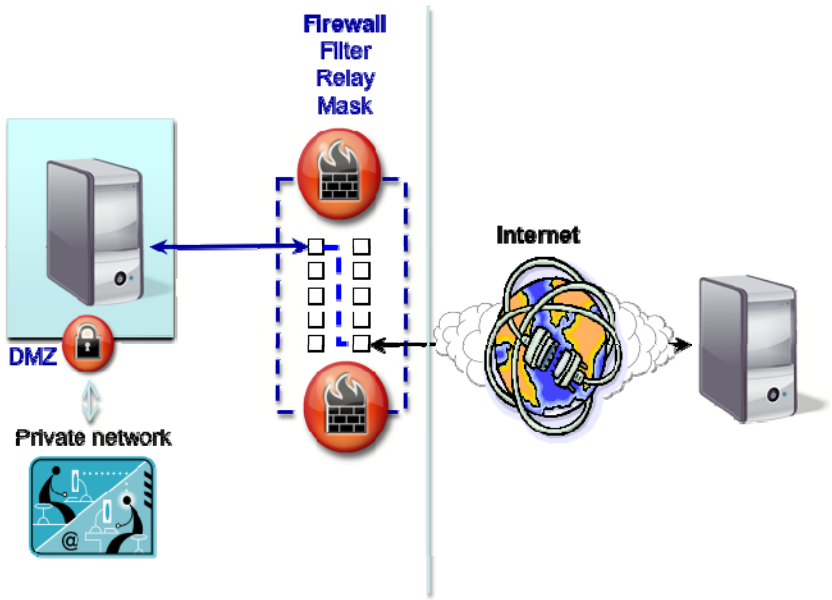

Figure IV.13: Functional structure of a firewall

Firewalls are generally categorized according to the kind of data and protocol filtering provided: IP, TCP, UDP, FTP, HTTP, etc. The type of firewall used depends on the nature of the analysis and processing to be carried out.

An *application firewall*, also known as a ***proxy*** (proxy server, proxy firewall), acts as an application relay. Operating on the user's behalf, it establishes the required service. The purpose of the qualified proxy system is to provide address masking by application relay and to make the organization's internal environment transparent. It serves as a mandatory crossing point for all applications requiring Internet access, and calls for the installation of a relay application on the user's workstation and on the firewall.

A firewall is only one of the hardware and software components used in implementing the security policy. A firewall on its own does not provide adequate protection. Implementing firewall is not enough to obtain a coherent overall security level. Other tools, measures and procedures, that are concomitant with the security objectives, should accompany a firewall installation. A firewall's effectiveness will depend essentially on its positioning vis-à-vis the systems it is to protect, and on its configuration and management.

IV.5 RISKS AND BASIC SECURITY MEASURES RELATED TO E-MAIL AND E-COMMERCE

IV.5.1 E-mail security issues and solutions

The electronic mail (e-mail) application is widely deployed all over the world for private or business uses. It facilitates the sending of non-structured information (the message itself) and documents (files attached to the message) across the network to any person having an electronic mailbox.

The risks of using an electronic mail system involve:

- Loss, interception, alteration or destruction of messages;

- Infection of systems through viruses in attached documents - within spam, for example. This constitutes the most widespread risk;
- Usurping of user identity: an intruder pretends to be someone else; an element of the system emits, listens to and intercepts messages for which it is not the addressee; this is the concept of masquerade/fake mail;
- Messages potentially being introduced, replayed, mixed up, suppressed or delayed;
- Denial of service;
- Interception of confidential information;
- Repudiation: an actor in the system denies having sent or received a message;
- Harassment, such as a flood of messages, or junk mail;
- All of the risks previously identified, linked to networks and their operational modes – such risks as attacks on routers or name servers.

Examples of risk associated with e-mail - Spoofed, fraudulent e-mails, that claim to come from the website of a well-known entity. The e-mail may attempt to redirect users to a malicious website. Often that malicious website will masquerade as the official website of the given well-known entity. Often it will install a Trojan horse designed to capture all typed information, including passwords, as soon as the user accesses some predetermined banking websites.

A variation of this scheme would be a fraudulent e-mail that claimed that the recipient had received a web card from a friend. The e-mail would include the link to download it, which would, of course take the user to a malignant site. Another variation would be a fraudulent e-mail that declared, "We have dedicated music for you". It would include a link to listen to the music. As soon as the user clicked on the link, he would be redirected to a bogus website where a *keylogger* could be immediately downloaded on his computer.

Cybercriminals can send a fraudulent e-mail that claims to come from a well-known anti-virus firm, The e-mail "warns" recipients that a worm has infected their computer. In order to remove the worm, users are requested to click on a URL address provided. This link redirects the users to a fake website hiding a malicious code that installs a keylogger designed to gather banking account information.

Because the content of the messages circulates unencrypted on the network[55], this limits the use of the mail system to the transfer of non-confidential data. Furthermore, the multiplicity of systems, networks, software, and the fact that there is no end-to-end connection when a message is transmitted, makes the security implementation of mail systems difficult. To offset this inconvenience, new versions of mail software integrate encryption features in order to ensure confidentiality, integrity and authentication of information exchanged between the correspondents.

Security needs for e-mail service are:

- Confidentiality;
- Availability;
- Integrity of a message or a sequence of messages;
- Non-repudiation: this involves the concepts of certification, electronic signature and certificates[56]);

55 A traditional mail system does not encrypt message content that is readable, and does not offer any guarantee of the authenticity of the message or its sender.

56 The UIT X.509 recommendation was the first standard to have specified the types of information contained in a certificate. It has contributed largely to the definition and the development of applications, such as mail systems or name servers.

- Authentication of the identity of all actors of the e-mail system; this includes users, intermediate elements, message memory, and message transfer agents.

The initial protocol of **Simple Mail Transfer Protocol (SMTP)** in the Internet environment has been enhanced over time to support multimedia contents and security mechanisms. Several are currently available. These include: (i) Secure Multi-purpose Internet Mail Exchange (S/MIME); (ii) Privacy-Enhanced Mail (PEM)[57]; and (iii) Pretty Good Privacy (PGP)[58].

Some e-security solutions consist of installing an *anti-virus* on each end-user system and on the mail server. However, users tend to deactivate them, because the anti-viruses slow processing time. Furthermore, an anti-virus only protects from the viruses it was designed for. It offers no protection from new forms of infection. The alternative comes down to implementing a server that systematically examines all the messages and their attached documents. Several anti-viruses can be used simultaneously, thereby increasing the probability of a corruptive message being detected.

Spam and malware propagation is a major concern for all parties involved in information security, including ISP, web hosting service providers, organizations, and individuals. It can spread over instant messaging (**spim**) and voice over IP telephony (**spit**). Fighting against spam requires an *anti-spam strategy*, *awareness*, and *international collaboration*. It requires both legal and technical solutions. In spite of the existence of several guidelines and best practices, spam remains a nuisance.

IV.5.2 E-commerce security issues

Electronic commerce is a commercial reality that represents considerable volumes of business. The cornerstones of e-business and e-commerce activities are security measurements and suitable procedures for marketing and selling on the Internet.

E-commerce security problems may arise for the customer at any of the following levels:

- The client system;
- The network infrastructure;
- The commercial server site of the company selling goods or services.

The risks to the customer are related to the disclosure or illicit use of confidential or private information, and to lures or malware infections. The problems of security at the network level are expressed in terms of degraded performance - prohibitive response times, incapacity to transfer the traffic, unavailability, dysfunction, routing errors, etc. A major risk for commercial enterprises is the unauthorized access to private servers through the Internet e-commerce server. That makes the enterprise vulnerable to a whole series of malicious actions and incidents, including robbery, destruction, and diversion. The potential consequences are loss of money, production, image, know-how, or competitiveness.

The security of commercial transactions depends on:

- A secure Internet connection between the customer and the salesman;
- A secure customer workstation;
- A secure data-processing environment of the salesman.

A secure Internet connection can be established between a navigator and a web server, by using SSL/TLS. The latter is integrated into the navigator, and ensures, in a transparent manner, that the coding of the data has been rendered confidential via cryptographic mechanisms. This establishes a

---

57 RFC 1421, 1422, 1423, 1424.

58 This solution is based on the IDEA algorithm for message encryption, MD5 for hash-coding of the summary, RSA for the encryption of the summary and the exchange of the private key necessary for IDEA. The latter is generated in a random manner at the time of encryption and is used only once. PGP optionally uses ZIP to compress the message before it is encrypted. The user's secret key or keys are memorised locally in encrypted form. This set of functions, which are executed in a UNIX, PC or Mac environment, is relatively easy to implement and well documented.

level of security that is sufficiently reliable to transmit sensitive information such as a credit card number to the network. In fact, the risk taken by the customer is no greater than the risk he would take while paying with his credit card in person.

Establishing a reliable way to transmit a credit card number confidentially is not sufficient to protect the commercial transaction. It is necessary to protect all sensitive information related to the transaction during the entire process. The salesman must ensure the confidentiality of sensitive information while it is being stored, and while the user is making requests for authorization of payment.

The principal credit card operators - Visa, Mastercard, and American Express - and many actors of the Internet world try to promote the deployment of **SET (Secure Electronic Transaction)**. This solution is based on the use of digital certificates and procedures of certification. It authorizes the global security of a commercial transaction in real time. SET requires the use of a public key infrastructure (PKI) to have the certification facilities, including the digital signature. The use of digital certificates guarantees the recipient that the electronic signature of a received document is valid. The major disadvantage of this solution, like all those based on the use of digital certificates, lies in the management, distribution, and validity of the certificates. All the actors of the commercial transaction must be registered with the same certification authority to perform trusted business transactions. The certification authority must be recognized, reliable, and independent. SET has been replaced by several solutions as for example (i) 3-D Secure (Visa); (ii) Mastercard Secure Code (Master Card) or (iii) J/Secure (Japan Credit Bureau).

To secure an e-commerce server, it is necessary to secure the server's information system, and to control the requests that the server receives. Beyond the strict configuration of a system called to lodge the e-commerce server, it is generally judicious to protect the system from outside with a firewall. A *firewall* is a system that can be placed at different points of the network to isolate and protect certain resources. The configuration of a firewall depends on the security criteria defined to filter the traffic. The information system security policy must define the configuration criteria before actual deployment. The tools and procedures established should be user-friendly, and authorize effective work methods. While it is essential to be able to limit access to data, it is also essential to ensure that data is readily available to authorized users. This can be achieved through effective software and configuration management, back-up procedures, systems and network dimensioning, resource redundancy and network management. All aspects relating to *user support* (help desk) and *customer assistance* (telephone support) may be regarded as part of the security of the server. Design, ergonomics, user-friendliness and facility of use are also important to support e-commerce services.

Beyond the organizational and technical aspects related to the installation of any commercial activity, it is important to be able to materialize the concept of a contract during e-commerce exchange. *Confidence* is the foundation of any exchange. Certification authorities can be used to accredit exchanges. These third-party organizations that intervene as guarantors in commercial transactions determine the success of e-commerce. Truly, the entire authentication process depends upon them.

The development of e-commerce is primarily dependent on the use of certification, which relies on *key public infrastructure* and on *legal aspects* related to immaterial transactions. Only the transborder and international dimensions of the electronic exchanges, which impose a coordinated strategy of certification and control at the international level, pose a problem for the deployment of e-business. Technical solutions exist; their implementation and use on a large scale must refer to a specific legal framework to prevent any abuse.

The effective management of information assets is essential in order to protect the individual privacy rights of the customer and the financial assets of the company proposing the e-commerce. An adequate insurance infrastructure must be developed in order to minimize the financial risks for every actor.

The security solutions for financial transactions over the Internet must offer the following services: (i) identification and authentication of the trading partners; (ii) data integrity and confidentiality during the transfer; and (iii) a service of no-repudiation. This involves infrastructure services that are based on public-key technologies, digital certificates and digital signatures.

Their effectiveness is dependent on the performance of certificate management facilities. Related problems concern: (i) the certification of certification authorities; (ii) the recognition of certification authorities; (iii) the interoperability of certificates issued from different certification authorities; and (iv) the validation of certificates.

The Internet is constantly evolving; the solutions of security must be adapted accordingly. However, Internet security is not the only barrier to the deployment of commercial activities on the Internet. Some actors take shelter behind the issues of security to justify their inertia with respect to the challenges of electronic commerce. They often use a technological or legal alibi to justify a kind of immobility. Reflecting globally on security questions and searching for good technological solutions make it possible to leave the risk at a very acceptable level – in any case, at a level comparable with the risk that comes with any commercial activity.

IV.6 PROTECTION OF COMMUNICATION INFRASTRUCTURES

IV.6.1 Some protocols communication security issues

To protect data during their transfer over an unreliable network, several security solutions alternatives can be implemented as for example:

- At the application level to secure the application protocols (S-HTTP, PGP, SMIME, etc.);
- At the transport level – for example, by SSL / TLS mechanisms to offer a secure connection between distributed entities;
- At the network level to secure the telecommunication infrastructure by implementing IPSec.

Figure IV. 14 summarizes the various alternatives of Internet security protocols implementation.

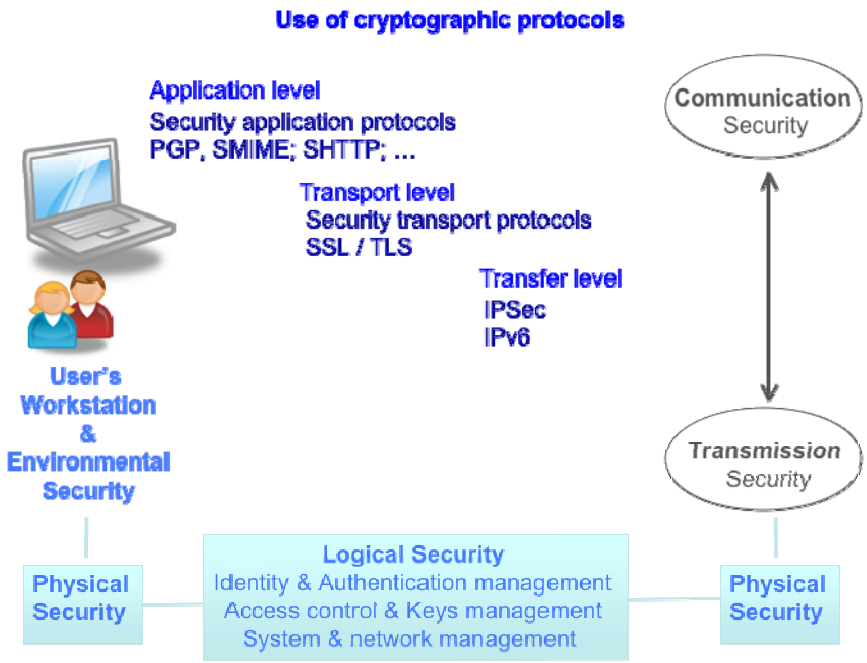

Figure IV.14: Protocols secuirty levels

Each of these solutions has its advantages and disadvantages. Whatever the security solutions are, their implementation affects the network architecture and the systems configuration, and they share the same security needs in terms of the following:

- Authentication of users or processes;
- Use of cryptographic mechanisms - the same algorithms must be used to encrypt and decrypt, the sender and the receiver must be able to negotiate the algorithm to be used for a given exchange;
- Effective key management;
- Formatting data, and transferring it to the right destination.

Security measures are also related to: (i) network configuration and management; (ii) operational system maintenance; and (iii) human resources management. Security technology alone is not enough - a robust cryptographic algorithm is ineffective if users divulge his secret keys!

Security technologies mainly depend on the following:

- An effective use of cryptographic mechanisms;
- Access control procedures;
- Secure communication protocols;
- Reliable hardware and software platforms;
- A non-permissive systems configuration;
- Good design and dimensioning of network architecture.

IV.6.2 Several levels of protection

Security of transmissions can be realized by producing *line scrambling*, i.e. by transmitting non-significant information in order to mask a flow of relevant data within an uninterrupted flow of unimportant data. However, it would be highly problematic if there were a need to protect transmissions against passive eavesdropping through capture of the electromagnetic radiation induced by the signal carried via the transmission media. If that event, the transmission media would have to be fully isolated in *Faraday cages*. Clearly, such a protection measure would be implemented only if absolutely necessary.

It is essential to properly set up and maintain the physical security of transmission media, hub, connection equipments, etc. The transmission infrastructure must be protected from any form of *radiation* that could compromise the data transmission process. It must be protected from passive attacks, such as data snooping, and active attacks, such as the modification, destruction or creation of data.

Knowing how to protect user connections is of paramount importance. To this end, the network has to identify the user, locate the user, and identify the requirements of the user. By responding to the general question "who does what and where", the network can identify the various security requirements pertaining to transport.

Securing the transfer of data comes down to integrating the security process into the communication infrastructure. Therefore, the latter must be capable of assimilating that process in its entirety. This usually requires the updating of all of the routers – a situation that can in some cases lead to problems of router interoperability and change management.

Encrypting data at the network level generates data packets that are larger than unencrypted packets, with the result that transfer occupies more bandwidth and communication resources. The encryption process increases the packet processing time. Therefore, the implementation of security at this level can have a *significant effect on network performance*. The main advantage of encryption at the

network infrastructure level is that it allows independence of the application and of the encryption mechanisms associated with the transfer, which are thus fully transparent for the user.

Implementing *transaction security at the application level* means that data is encrypted as close as possible to the data−handling application. This modifies the application itself, because the data is encrypted upstream of its delivery to the network protocol that will route it to its destination. A session key is authenticated and negotiated during the dialogue set-up phase between the application entities. The complexity of this phase can vary, and the establishment time varies proportionately. Once this phase has been completed, encryption is generally quite rapid. It is independent of the execution platform and communication infrastructure.

Protection at the level of the work sphere of a user implementing a distributed application no longer depends on the data carrier or network. It now depends on the user's immediate environment.

The difficulty of protecting applications lies in the fact that the protection afforded has to encompass the following:

- The entire application environment;
- The user's workstation;
- The user's physical environment.

Protecting applications comes down to the question of individual user rights in regard to workstations, applications and the physical area within which they operate.

The basic functions of the operating system installed on the user's workstation play a prominent part in the following:

- Preventing other parties from taking control during a session;
- Preventing automatic disconnection after a certain period of time;
- Protecting network cards;
- Providing secure−mode support for application protocols, such as the transmission of protected files, and secure messaging;
- Mirroring and duplexing operations, such as protecting data by duplicating them on disks, and performing write−operation and equipment redundancy.

Securing the transport infrastructure or securing the application comes down to addressing the same issue at different levels:

- Authenticating the processes and users;
- Ensuring that the sender and the recipient use an identical encryption/decryption algorithm;
- Ensuring that each communicating entity is in possession of the algorithm and the encryption/decryption keys;
- Managing the encryption/decryption keys;
- Formatting the data prior to transfer.

IV.6.3 Systems and network management tools for security enhancement

When properly implemented, system and network *management activities* can ensure the levels of availability and performance that are necessary to achieve security. Those activities include network surveillance and anomaly or incident detection – tasks that make a major contribution to the overall security of the network and of the information system it serves.

Good network management helps to keep infrastructures, services and data available with a *high degree of efficiency*. Through *network management* - particularly configuration, performance and incident management - it is possible to ensure availability and integrity.

Furthermore, the aspect of network management known as accounting management makes available all of the data necessary not only for invoicing users but also for performing essential surveillance and audit functions. This can serve in the verification of actions in the context of proof or of non-repudiation.

Network management also contributes to achieving the confidentiality objective, insofar as it ensures the absence of snooping or unauthorized access to the data. The access control function that is a component of network management is essential to the operational implementation of security.

The performance, quality of service, availability and reliability of a network depend to a large extent on:

- How well routers are managed;
- How effective are the facilities that control route switching.

Updating the routing tables of major networks is a real operational headache for network administrators. Any changes to the values in the tables must be synchronized in order to avoid malfunctioning and loss of data in transit. The network management protocols are designed to enable the updating of routing tables.

Network management can contribute to router security by:

- Establishing secure access points during their configuration;
- Generating alarms in the event of intrusion attempts;
- Securing the router management and monitoring centers.

In order to prevent unauthorized individuals from introducing changes, it is crucial for network managers to be able to provide the necessary protection by blocking or detecting the following actions:

- The modification of addresses contained in routing tables, IP packets, etc.;
- The modification of routes and illicit copying of transported data;
- Flow monitoring;
- Diversion, modification and destruction of data packets;
- Denial of service, router attack, network flooding, etc.

It is important to be able to *secure the processes* whereby data are routed through telecommunication networks. Network service providers must protect all entities involved in this process, particularly routers and name servers. The quality of the routing service must meet the security criteria of availability (the service is operational), confidentiality (the data are delivered to the right recipients) and integrity (the data are not modified during transfer).

A network service does not guarantee the delivery of data to authorized parties. The delivery service does not verify that data delivered to a given address are actually delivered to the parties authorized to receive them. This would require an additional check of the "access control" type. Moreover, if the data are sent without encryption, and are tapped into en route, they will be intelligible to unauthorized third parties. It is important for sensitive data to be encrypted.

Monitoring of an information network requires constant observation of its functioning. In addition to ensuring an acceptable level of service, effective monitoring ensures the detection of problems, incidents, errors and anomalies that degrade network performance and could jeopardize the security of the resources. In the sphere of auditing, network monitoring allows for the tracing of actions and events, so that they can be logged for subsequent analysis. It also helps to ensure resource availability by verifying that the network is functioning correctly. Therefore, it is therefore a crucial function within the framework of network management, since it plays a part in performance, incident, configuration, user and security management.

IV.7 TOOLS ARE NOT ENOUGH

Security must be approached in a global manner. This involves the implementation of procedural measures as well as the use of appropriate tools. Tools alone cannot solve an organization's security issues. If they are managed in a disorganized fashion and are poorly integrated within a continuous process, they will only hinder usage, load operations and hamper the information system performance.

A defined architectural framework, in the context of a global approach to enterprise security, provides a clearer vision of the general dimension of information technology security. The organization can then develop the different components in a coherent and harmonious manner. Moreover, the existence of a security referential facilitates the evaluation of the existing state of system security and its audit.

The design of a secure digital distributed environment depends on the definition of a conceptual framework – a **security architecture** - within which individual security components can be developed.

Figure IV.15 represents the different organizational, human, regulatory and technical aspects involved in ICT architecture security. This architecture allows for a **systemic approach** that enables the identification of: (i) minimum security to be implemented for each element; and (ii) the possible incompatibilities of the different security levels of the individual elements. A well-considered systemic approach toward the security architecture ensures a global coherence of security measures, process and tools.

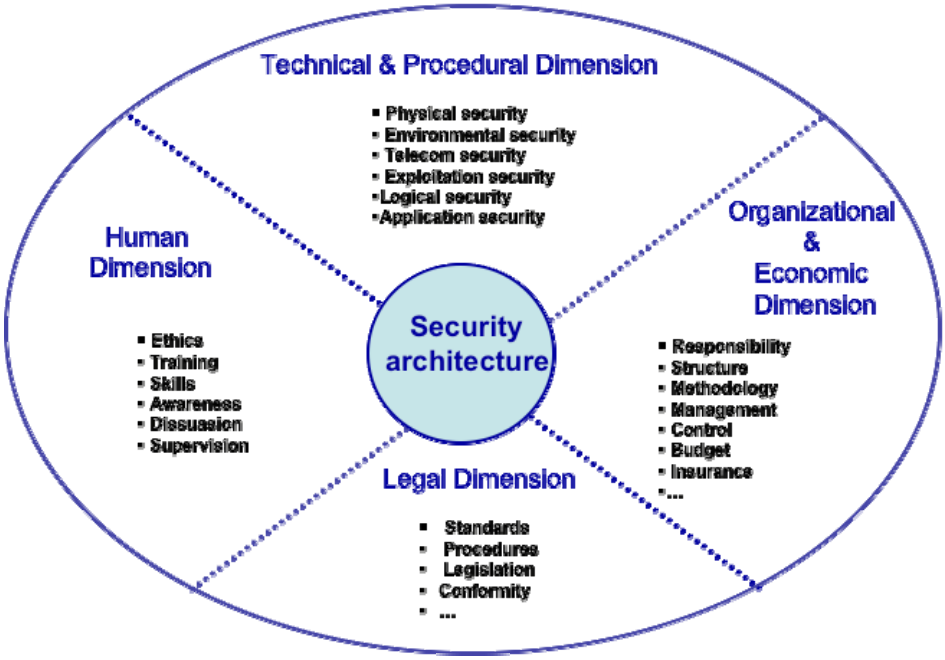

Figure IV.15: Different aspects of security architecture

Security measures should be updated in regard to evolving technologies and the accompanying risks. Security must be proportional to the risks incurred, and must be implemented only to protect values that are actually under threat. A security manager must search for a balance between relevance and performance. Security measures and procedures are coherent when they are optimal yet simple – when they allow for an acceptable performance level and an ergonomic usage of computer and telecommunication resources.

PART V

MANAGERIAL APPROACH

Part V focuses on managing risks and security in a context of business intelligence. It contributes to understanding how to build a cybersecurity strategy, define a cybersecurity policy, and implement security measures.

The objectives of this part are to:

- Define the information security mission and success factors;
- Identify constituent elements of a security strategy and policy;
- Present a global approach for controlling information technology risks & security governance;
- Define security measures with a special focus on protection against system intrusion, crisis management, and disaster recovery plans;
- Propose an organizational structure for security management;
- Indicate the principal criteria for auditing and evaluating security levels.

V.1 SECURITY MANAGEMENT OBJECTIVES AND DEFINITION

V.1.1 Security is a business enabler

The objective of **information systems security** is to guarantee protection for the organization. This consists of: (i) reducing the likelihood that threats will occur: (ii) limiting the number of vulnerabilities and incidents; and (iii) enabling a return to normal operations within an acceptable period of time and at affordable costs.

The type of incidents include: (i) human error; (ii) natural disasters and accidents (such as flooding and fire) and (iii) criminal and malicious action (such as theft or vandalism). *Security might not bring monetary gain but it does prevent monetary loss.*

Organizations and states can develop services capable of stimulating an economy by having a good cybersecurity approach. It is no less than a *defensive strategy* that is part of an **economic intelligence approach** (Figure V.1)

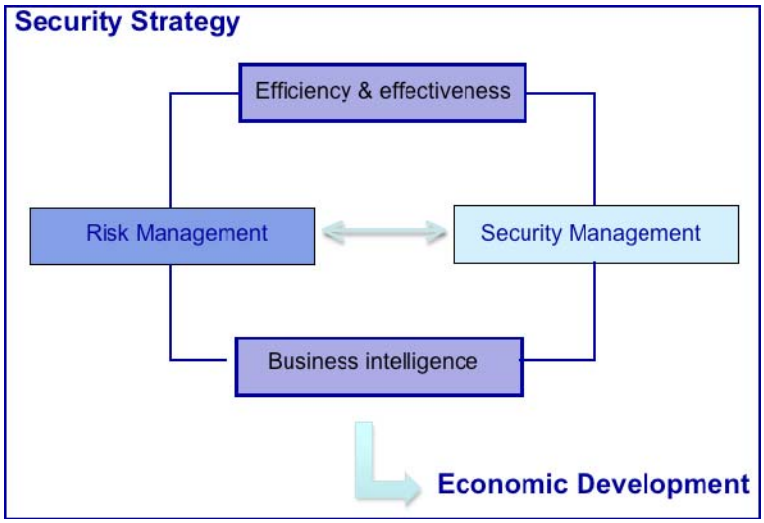

Figure V.1: Main cybersecurity objectives

Security and quality approaches share the common goal of providing process, information and services for which quality is guaranteed (Figure V.2).

Figure V.2:Complementarily of security and quality approaches

An organization creates information technology security through *rigorous management* of logistics, human resources, information systems, workplace sites and environmental infrastructures. This includes control of the power supply, natural risks and respect for legal and regulatory provisions. Cybersecurity management is above all a matter of linking security tools and services to the system's operational administration. Tools, such as encryption and firewalls, cannot adequately ensure protection unless they are an integral part of a precise *management process* and are accompanied by procedures that govern their use.

Security depends on *complementarities* between the managerial, technical and legal aspects. These aspects need to be handled in parallel. *Security is never definitively acquired.* The constant evolution of information systems and risks means that all security measures are transitory. Therefore, security management must be a *dynamic process* — one that is constantly evolving to counteract the evolution of security risks.

V.1.2 Security is a endless and dynamic process

Achieving security is possible through managing a dynamic and endless process that requires several capabilities and competences (Figure V.3).

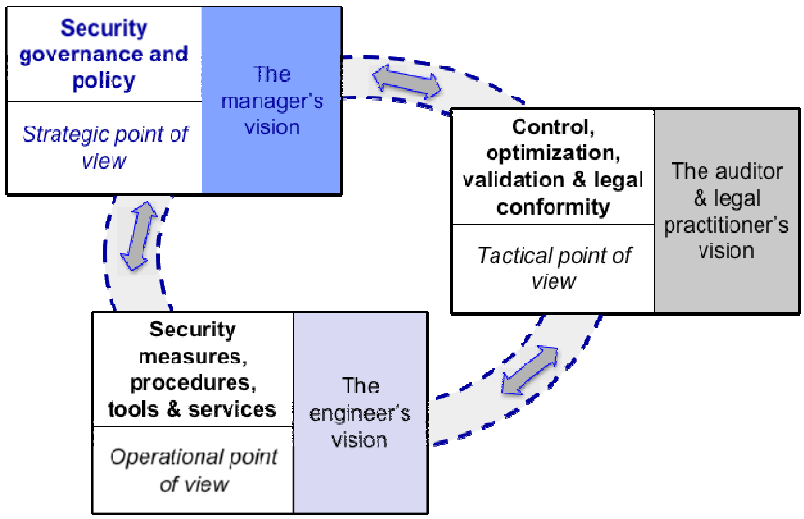

Figure V.3: Security: an endless process requiring several capabilities

Global security efficiency does not just depend on security tools. It also depends on a *coherent strategy* and the application of a complementary set of procedures. This requires *an adequate structure control* through which the organization can successfully manage, implement, validate and control security measures.

The responsibilities and the appropriate security procedures and directives should be well specified. The structure control must be coherent with the enterprise and information technology plans. To this end, a strategic vision of the global security is necessary.

A security policy must offer a graduated response to a specific security problem in regard of a particular risk situation.

The choice of security measures to be implemented is determined by making a trade-off between the cost of the risks and the cost of their reduction, and by balancing the *need for production* with the *need for protection* (Figure V.4). This involves short, middle and long-term analyses of security requirements and means.

Figure V.4: Security: a necessary compromise

V.1.3 Security is a question of principles

The following fundamental principles facilitate the implementation and administration of information technology security in an organization:

Vocabulary principle: There is a need to agree, at the organizational level, on a common language to be used in the field of cybersecurity.

Coherency principle: An accumulation of security tools is not sufficient to achieve a global and coherent security structure. The security of an information system is the result of the harmonious integration of tools, mechanisms and procedures relating to prevention, detection, protection and correction of damage caused by error, malicious intent or natural elements.

Management engagement principle: It is the management's responsibility to provide the necessary means for the implementation and administration of a security plan. This principle results directly from the consideration of information as an organization's strategic resource.

Financial principle: The cost of security and the control measures must be proportional to the risk.

Simplicity and universality principle: Security measures must be simple, flexible, and understandable and applicable to everybody.

Dynamic principle: Security must be dynamic in order to integrate the time dimension and the changing requirements.

Continuum principle: An organization must continue to function even after an incident. This requires emergency and recovery procedures.

Evaluation, control and adaptation principle: An organization must set up the measures, procedures and tools that allow for a permanent and dynamic assessment of the security level of an information system. This enables the organization to have a better understanding of: (i) the variability of the security criteria; and (ii) the adequacy of the present level of security compared to real security needs, which are by nature evolutionary.

The following points constitute the main conditions of success for a security approach:

- Management support and implication is required;
- Simple, precise, understandable and applicable (feasible) security policy;

- Dissemination of the security policy among all the stakeholders;
- Trained, reliable and aware personnel with high moral value;
- Expression, control, respect and validation of security clauses in contracts; business ethics regarding legal constraints;
- Procedures for backing-up, recovering, monitoring and auditing;
- Human Rights respect and proportional security answer;
- Determination to avoid dangerous situations.

V.1.4 Security is a question of perspectives

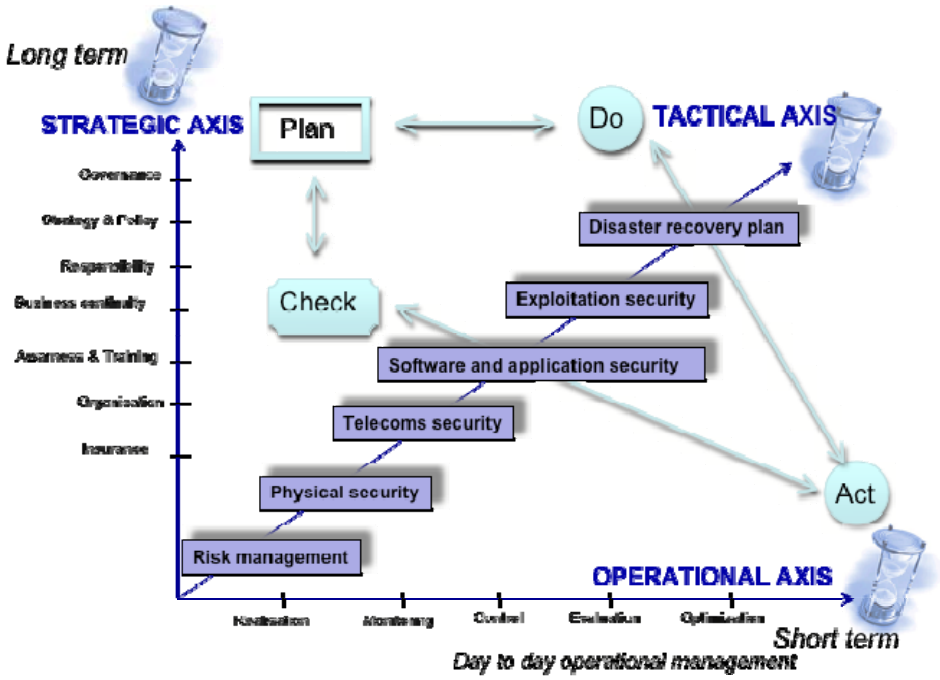

Figure V.5: Strategic, tactical and operational security aspects

Figure V.5 presents a cybersecurity approach from a long-term perspective to a short one. The **strategic or long term axis** is represented vertically. It consists of generalized directives that are determined by the organization's security policy. The **operational axis** is represented horizontally. It consists of generalized tools for a day-to-day operational management. The **tactical axis** (or middle term) is represented diagonally. It consists of generalized measures to be realized by specific technological and procedural measures. The organization determines what kind of measures to take (tactical level) by assessing how the tools available can best be utilized to achieve the directives specified by the strategic level.

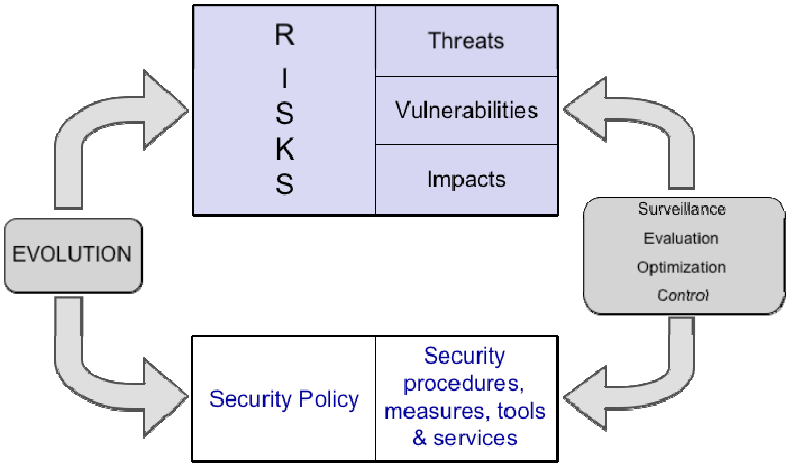

Figure V.6: Risk and security in a dynamic context

The security approach of an organization's information system integrate the following points belonging to a virtuous circle (Figure V.6):

- Defining the vulnerability perimeter related to the use of information and communication technologies;
- Offering a level of protection that is adapted to the organization's technological risks;
- Realizing and validating the organizational and security technical measures, tools and procedures;
- Optimizing performance of the information system according to the security level required;
- Ensuring reliable information system and security evolution conditions.

V.1.5 Security is a question of governance

The goal of *security governance* is to ensure that organizations use the most suitable security measures at each given place and time. This concept revolves around the following simple questions:

- Who does what, how and when?
- Who are the players who develop the rules, define and validate them, implement them and exercise control over them?
- Who controls the security?

Approaching security through a dynamic and continuous management process positions an organization to deal with the dynamic nature of the security risks, by continuously adapting and improving its solutions. The quality of the security management will determine the level of security provided. Cybersecurity policy should be defined at the level of top management. There are as many security strategies, policies, measures, procedures and solutions as there are organizations with security needs that need to be met at any particular time.

Consider, for example, the process of detecting and patching security vulnerabilities. This consists of periodic issues of security patches. Information newsletters, more or less customized, make it possible for concerned persons to stay informed about perceived vulnerabilities and methods for patching them up. If the organization is to maintain a minimum level of security, the security or system administrator will have to install the security patches as they are issued. However, knowledge of dangerous system vulnerabilities is useful not just to the security administrator, but also to hackers, who may attempt to

exploit them before the patches have been applied. It is therefore imperative to continuously update the security solutions, and thereby *maintain a consistent level of security*.

Published alerts and patches allow the administrator to control the update process (by choosing whether or not to install those patches). It is also possible to put the update process into automatic mode, effectively delegating the responsibility for regular and systematic patch installation to the software publisher.

This raises the question of *responsibility*. What are the legal consequences of a software update that has been declined, when problems arise from the exploitation of an uncorrected vulnerability? Since numerous attacks do just that, the question of who has responsibility is crucial.

The dynamic dimension of security represents a crucial challenge not only for the providers of security tools and software publishers, but also for system and security administrators, who rarely have the time needed to incorporate all of the patches and updates that are available.

Computer managers, security administrators and system administrators possess full access to the organization's ICT resources. Therefore, the organization must apply strict surveillance and control procedures for their activities, proportionate to the risks to which these individuals potentially expose the systems under their control. The organization must also ensure that staff has irreproachable personal integrity.

Service providers who offer anti-virus and anti-spam filters effectively take over a part of the security management for their customers. This trend is starting to change the distribution of roles and responsibilities in security matters. Security will increasingly be shifted onto the service provider or technical provider. Of course, this shift does not resolve the problem. It merely transfers it to the service provider, who becomes responsible not only for the availability and performance of the service, but also for the management and maintenance of a certain level of security.

Publishers of anti−virus software typically offer an automatic update service. The addition of this new dimension of service makes software rental increasingly attractive, because the responsibility for maintenance is transferred to the publisher for a lengthy period. It also fuels a broader trend towards the outsourcing of applications, and a concomitant business model.

The question of **outsourcing** or delegating all or part of the security mission is not purely technical. It is also strategic and legal, and raises the fundamental issue of **dependence** on suppliers.

A **security outsourcing strategy** may include:

- The definition of policy;
- The implementation of policy;
- Access management;
- Firewall administration;
- Remote maintenance of systems and networks;
- Third−party application maintenance;
- Back−up management.

A quality-control process must accompany the choice of a contractor, It may take into account such things as: (i) experience; (ii) in−house expertise; (iii) technologies used; (iv) response time; (v) support service; (vi) contractual arrangements (e.g. guaranteed results): and (vii) sharing of legal responsibilities.

V.1.6 Security is a question of measures

Security prevention is, by definition, proactive. It involves the human, legal, organizational, economic (ratio between implementation cost/level of security/services offered), and technological dimensions.

As of now, ICT environment security has concerned itself largely with the technical dimension. This way of understanding information systems security, emphasizing the technical dimension to the neglect of the human dimension, creates a serious problem in controlling the technology risk associated with criminal acts. Crime and delinquency are primarily a human issue, not a technical one. Therefore, a purely technical response is inadequate.

The typical approach toward ICT related crime is one of reaction and prosecution. Therefore, action comes after the occurrence of an incident, which, by definition, has highlighted a gap in the protective measures. An organization needs: (i) to prevent and deter cyberattacks by developing investigative/criminal mechanisms, and (ii) to identify those measures that are needed to respond to attacks and prosecute the attackers. It must design and implement back−up and continuity plans, incorporating the constraints related to the investigation and prosecution of cybercrime within the different work processes and objectives, with specific time−scales.

From data, software and services perspectives, protection needs implies that the following security properties must be assured by technical and procedural measures:

- **Confidentiality** (no illicit access) - keeping information secret by giving access only to authorized entities;
- **Integrity** (no falsification) - keeping data integral without alteration;
- **Accuracy** (no errors);
- **Availability** (no delay) - maintaining uninterrupted access to services and data without degradation;
- **Durability** (no destruction) - maintaining data and software applications for the necessary duration;
- **Non-repudiation** (no objection).

Security measures must guarantee these properties in proportion to the value and life cycle of the information. Tools with specific capabilities and persons with specific skills are required to implement those measures. Sound administrative and audit procedures are required to manage and validate them. Cybersecurity depends on a *coherent set of measures, procedures, people and tools*.

Figure V.7: Security measures

The following are categories of security measures (Figure V.7):

1. **Preventive measures**, such as logical and physical access control, and virus detection - their role is to ensure that an attack does not succeed;
2. **Dissuasive measures**, such as legal and administrative procedures, awareness training, management of human resources, work conditions, and means of detection and tracing - their role is to discourage criminals from making an attack;
3. **Structural measures**, such as masking resources, redundancy, and information fragmentation - their role is to protect the organization values;

4. **Protective measures**, such as coherence checks, intrusion, fire, humidity and transmission error detection, and firewalls – their role is to block attacks and to limit the effect of any incidents that do occur;
5. **Recovery measures**, such as insurance and lawsuits – their role is to limit losses following an incident.
6. **Palliative or corrective measures**, such as backup, continuity plans, redundancy, repair, and correction – Their role is to repair damage caused by an incident;

V.2 IDENTIFY AND MANAGE ICT RISKS

Cybersecurity risks are those associated with information processing, telecommunication and cyberspace. They are also referred to as computer risks, information risks or technology risks. A solid analysis of these risks must inform the security strategy for digital infrastructures. They need to be identified along with the strategic, social, and environmental risks facing the organization.

ICT risks are operational by nature. A sound analysis of security needs makes it possible to define a security strategy and security policy. The process of making this analysis revolves around the following questions:

- Who will be in charge of the risk analysis and risk management?
- What is the best way to conduct risk analysis?
- What tools and methods are available? How reliable are they?
- How much emphasis will there be on results?
- What are the costs?
- Would it be better to outsource this function?

V.2.1 What is a risk?

Risk may be defined as a *danger* that can be anticipated to some extent. It is quantified by the likelihood of damage and the resulting harm. Risk expresses the probability of an asset or value being lost due to a *vulnerability* connected with some hazard or danger.

In deciding on the desired level of protection and the types of security measures to put in place, it is necessary to balance the magnitude of the risk (in financial terms) against what it would cost to reduce it. At a minimum, the organization must identify the assets to be protected, along with the rationale for protecting them. The strategy will depend on actual constraints and the available organizational, financial, human and technical resources. The measures taken must be effective, and must reflect a balance between performance and cost-effectiveness.

Mastering ICT risks means elaborating a risk management strategy, defining a security policy and deciding on its tactical and operational implementation.

A risk can be viewed as a function of three variables:

- Threat;
- Vulnerabilities;
- Impact.

For an organization, *mastering information technology and informational risks* implies the definition and implementation of a *security policy*. Whatever the method used to specify a security policy, the objectives remain unchanged. The mains steps for defining a security policy are:

- To identify values, the level of vulnerability linked to specific threats and potential losses associated to risks (what is to be protected, against whom, and why?);
- To implement preventative measures (i.e. tools and procedures that minimize risks);
- To implement corrective measures (i.e. recovery procedures in the case of an incident);
- To implement an audit process, through which to check the pertinence and coherence of the security policy and the appropriateness of the tools used.

V.2.2 From risk analysis to security policy and measures

The *risk analysis phase* is very important to the process of determining what preventative security measures should be implemented (Figure V.8). Mastering information technology risks means reducing them to an acceptable level for the organization.

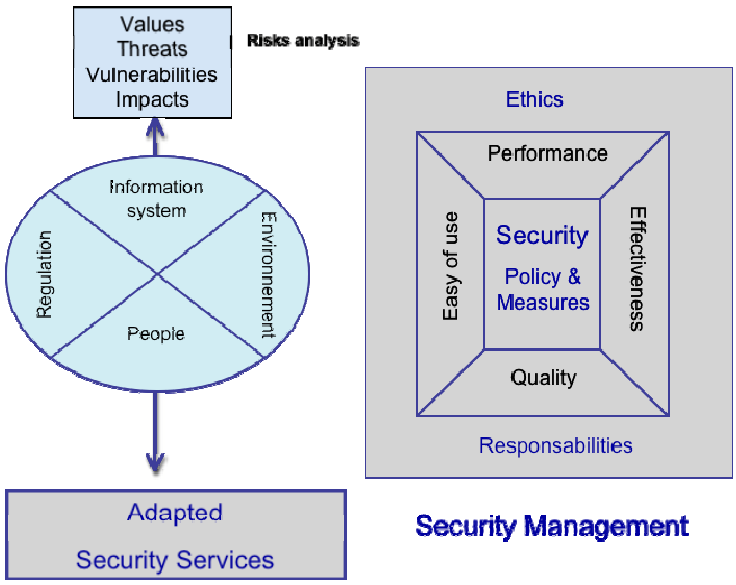

Figure V.8: From risk analysis to adapted security services

Security organization is specific to an institution's organizational structure. There are as many security policies and tools as there are organizations and security requirements. A security policy must offer a graduated response to the specific security threats that have been identified during the risk analysis phase. Management is responsible for the evaluation of risks, the definition of a security policy and the implementation of the organizational structure to support that policy. Risks and policies must be the object of constant evaluation and update. Therefore, the securing process includes risk analysis, prevention, reaction, verification and validation steps (Figure V.9).

The security approach is an *organizational project*. It is similar to the concept of total quality in that it concerns each and everyone. Developing an institutional *security ethic* will enable the organization to reinforce the validity of its security approach.

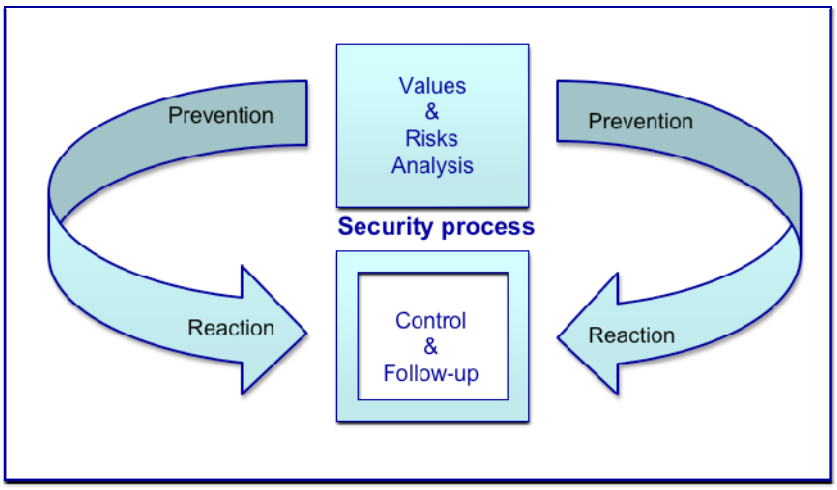

Figure V.9: Risks and the security process

The following questions are relevant for the development of a security approach:

- What are the real risks?
- Are these risks tolerable?
- What values need to be protected?
- From whom do these values need to be protected?
- What is the current security level?
- What level of security must be reached?
- What are the effective constraints?
- What are the available means (money, skills, resources, etc.) for achieving the desired level of security?
- How can the necessary security measures be implemented?

An organization defines general security norms or security references or rules that are common to all of its members. These norms concern for example: identity management, access control, permissions, etc. The organization must also stipulate what the security demands are regarding external partners.

The organization must identify:

- Technical and organizational constraints. This is necessary in order to determine the technical and organizational feasibility of the security policy for each objective;
- Inherent and applicable security resources and mechanisms. This includes configuration, parameters, user administration, and the like.
- The risks and the possible scenarios of an incident. This includes usage and parameter errors, accidents, malevolence, sabotage, software attacks, and the like.

V.2.3 Define a security policy and implement appropriate solutions and procedures

The security policy translates the organization’s perceptions of the risks and their impact into security measures for implementation. It facilitates both prevention and remedial action in response to security

problems. While it is impossible to eliminate risk entirely, and difficult to anticipate all the emerging threats, it is important to reduce the vulnerability of environments and resources that are to be protected.

An organization should not measure the effectiveness of a security policy on the basis of budget size, but rather, on the quality of the risk analysis and of the risk-management policy. The quality of cybersecurity depends primarily on (i) identification and evaluation of the information assets, (ii) operational deployment of appropriate security measures based on a well−conceived security policy; and (iii) effective management.

V.3 A STANDARDIZED APPROACH TOWARD SECURITY MANAGEMENT

V.3.1 Use international standards

A *security policy* is a set of rules and directives that are designed, on the basis of a *risk assessment*, to minimize the likelihood of an attack; and to repair the damage in the event of an incident. The former are called preventive measures, and the latter corrective measures. ISO information security standards–related presents a number of recommendations or controls to be implemented. According to ISO 17799 and ISO 27000 family standards, the purpose of information security is to ensure business continuity and minimize business damage by preventing and limiting the impact of security incidents.

ISO/IEC 17799:2005 (Information technology – Security techniques – Code of practice for information security management) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance.

The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 17799:2005 is intended to be a common basis and practical guideline for developing organizational security standards and effective security management practices that will help build confidence in inter-organizational activities.

ISO/IEC 17799:2005 proposes recommendations intended for the persons in charge of the definition, implementation and maintenance of an organization’s information security. It defines information security as the protection of the availability, integrity and confidentiality of the information assets whether in written, spoken or digital form. That is to ensure business continuity and damage reduction, but also to maximize the return on investment of information systems. The ISO 17799 standard

provides an approach to plan out suitable policies, procedures and controls, in order to better manage information technology risks. This process is balanced between the following types of security: physical, technical, procedural, and human-related. This standard is applicable to:

- Informational assets, such as files, databases, records;
- Physical assets, such as servers, PC, laptops, and computer hardware;
- Software assets;
- Assets related to the services, such as informatics and communication departments, general services, and the power supply.

The other standard applicable to information security management is ISO 27001:2005 (Information technology -- Security techniques -- Information security management systems – Requirements).

ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of an organization's overall business risks (Figure V.10). It contains recommendations for the implementation of security controls. These recommendations are customized to the needs of individual organizations or parts of organizations. It is designed to ensure the selection of adequate and proportionate security controls that protect information assets and provide confidence to interested parties.

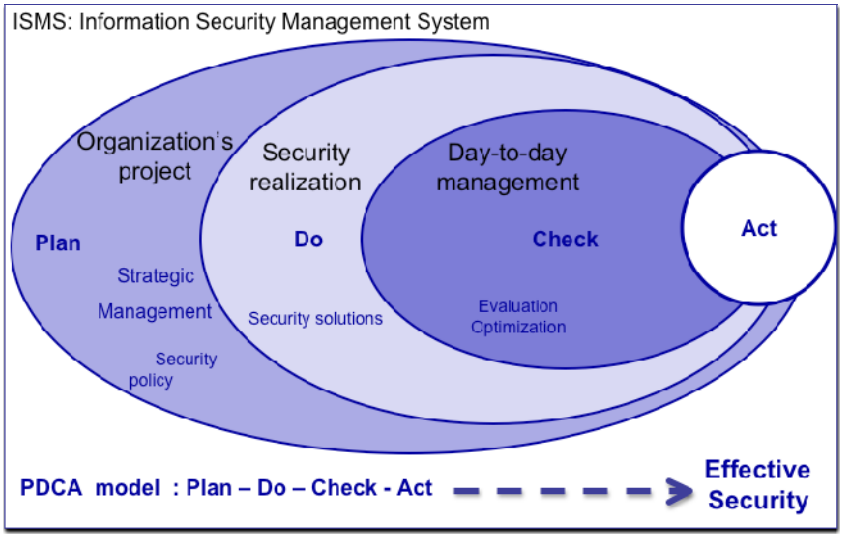

Figure V.10: Information Security Management System

Developing an **Information Security Management System (ISMS)** meeting ISO's 27001 requirements implies having three stages:

- *The first stage* is related to the *creation of a managerial framework* for the information system. It is about fixing the directives, intentions and objectives related to information security, and planning out the strategic policy of the top management.
- *The second stage* is related to *the risk identifications and evaluations* undertaken in order to define the proper managerial actions to undertake. The aim is to fix priorities to control the information security risks.
- *The last stage* is related to *the development of an Information Security Management System*, and, therefore, to the selection and implementation of controls. Once the requirements

are identified, adapted controls can be selected. These controls must ensure that information technology related risks are assessed and mitigated – those risks must then be reduced to an acceptable level. These controls involve policies, practices and proceedings related to the organizations' structure.

Phase 1: Creation of a managerial framework

An organization's project:

- Defines a security policy;
- Assigns responsibilities to the competent staff members possessing the authority and necessary means;
- Mobilizes all employees (alert, inform, train);
- Identifies security targets for each area (software, hardware, and organizational) in the information system requiring a certain level of security;
- Defines the issues – assesses the relative importance of each target;
- Outlines the potential threats for each target;
- Indicates the security level of each target;
- Estimates the gaps in the security system.

This last item is as important as the results of the analysis that guide the security choices for the whole of the enterprise.

Security management implies data classification and identification of data properties. An efficient classification system indicates the degree of protection required for each datum. The organization must designate specific procedures for delivering and cancelling resource access authorizations. It should not overlook the establishment of reporting and supervision procedures for information system activities.

Phase 2: Quantification and implementation of security measures

One approach of information technology security is to describe what is expected of the component elements of the information system architecture. This process generates valuable recommendations that must subsequently be validated by management. Next, security rules are broken down into tools, mechanisms and procedures that are required to reach the security levels set for each target area. This includes the following:

- Physical;
- Network;
- Data and software;
- Application development;
- Documentation;
- Maintenance and operations;
- Security administration;
- Human resources management.

Phase 3: Day to day management and validation of the measures

Once the measures are established, their appropriateness and efficiency must be verified in order to test, validate or adapt them, if necessary.

A security audit authorizes the evaluation of the *global coherence* of security solutions in regard to the stated objectives.

The active audit of a network makes it possible to see exactly what is happening inside; it contributes to the monitoring of the network's behavior. This provides a proactive overview of the constituent elements of the network and their operating mode, so that the organization can react dynamically to dangerous situations. This includes audit of connections, detection of possible intrusions, and file logs analyses. This approach is usually integrated into network management. The progressive installation of the network's history through the systematic memorization of events constitutes its operational life's memory. The organization can use this recorded information in log files (statistics, connections frequency, use of resources, etc.) to obtain a better understanding of the conditions surrounding an incident occurrence. Consequently, it can adopt appropriate security or network management policies. Beyond the simple technical reconstitution, this history makes it possible to prove the reality of some events, and sometimes even the identity of their authors.

Cybersecurity is lived out on a daily basis and is never acquired definitively. It should be continuously adapted, according to the evolution of technologies, needs and risks.

Audits make it possible to evaluate the security level of a given environment, and to measure any variations from the desired level. Thus, audits contribute to identify the steps and security actions that an organization needs to undertake.

Audit procedures evaluate and verify that the security level of each target conforms with those defined in the security policy. They must be done periodically in order to guarantee the adequacy of security means and tools to real risks.

A technological security survey can be seen as a *continuous audit process* of general security risks and market solutions. It falls under the step of anticipation of security requirements and solutions, and is related to the strategic, tactical and operational security aspects. It allows the company: (i) to remain vigilant; (ii) to identify potential threats before they occur; (iii) to discover new software faults; and (iv) to determine the signature of acts of vandalism.

V.3.2 Use common sense

The definition of a security strategy and its translation into security policy make it possible to identify the level of security that the organization must attain. It is then possible to translate those specifications into *concrete actions and measures*, by establishing the most suitable technological, organizational and procedural tools. Security is above all a matter of common sense (Figure V.11).

Figure V.11: ICT security: a matter of common sense

V.3.3 Minimize the cost of security

In the interest of cost effectiveness, it is prudent to secure only strictly essential resources.

The inherent costs of a security approach vary according to the following:

- The architectures of the information system and the concerned networks;
- The organization and structure of the organization;
- The reliability of the components of the information system and employed technologies;
- The nature and quantity of data and informational flows to be protected;
- The presence of an inventory of all the ICT resources and an effective resource management process;
- An assessment of the security needs in a given context of activity and business.

There are several actions to be carried out in-house, before the intervention of security experts, that contribute in *reducing the costs of a security system*. This involves correctly identifying the following elements:

- The data processing and telecommunication environments of the organization - hardware, software, data and programs, distribution, flows (source, recipient, and telecommunication technology, etc.;
- The participants in the information system, including persons, responsibilities, sites, and missions;
- The existing level of security;
- The required level of security.

In order to minimize the cybersecurity costs, an organization has to:

- *Concentrate on high-risk areas* in order to identify the threats that can paralyse the company's core business. This helps the organization to think about security in a business context, instead of undertaking security just for the sake of it;
- *Focus on opportunities* to implement high-profile projects that increase the value of the information system brand. Security is not simply about risk avoidance. Numerous security projects can result in significant cost savings for the entire business, and can also enable business to function in a way not otherwise possible;
- *Concentrate on operational efficiency* - look at what is consuming time, money and human resources. Elimination is the process of determining and removing unnecessary procedures, technologies or resources that do not add value to your security position.

Insuring against risk is an *economic protection* measure and not a preventive measure. It is a pro-active measure and a complementary action, which helps minimize the financial losses caused by a disaster. The insurance policies for electronic and data processing installations generally cover deterioration or destruction occurring suddenly and without warning. They cover damage resulting from an external event caused by the following:

- Manipulation errors or negligence;
- Conscious prejudicial acts;
- Upsets or falls;
- Atmospheric pollution and foreign bodies;
- Effects of humidity and temperature;
- Overloads;

- Vibrations;
- Fires or explosions;
- Natural disasters, such as storms and flooding;
- Loss through theft.

Risks may originate from several different factors, and be of different types, including specific information technology risks, and general risks, such as a fire that affects information technology. *Not all risks are insurable.* The organization needs to accurately assess the value of the object to be insured. This presents the complex problem of quantifying the value of the information, and the amount to be disbursed for a future potential claim. This is a classic problem for the actuarial sciences. Premiums are calculated on a case-by-case basis, as a function of multiple factors, and are often expensive and subject to numerous restrictions. It is regrettable that insurance companies do not offer bonus systems when organizations implement effective security measures.

Insurance policies usually cover hardware damages and data loss. This concerns the value of all the elements (when new) mentioned in the policy, and the costs related to continuity of operations after a disaster. However, because *it is difficult to estimate the financial value of information*, and of all the related economic consequences, insurance policies only cover the cost of information reconstitution provided the organization can prove that some external action actually resulted in its disappearance or alteration. In developed countries, insuring information technology infrastructures and security is a major issue that still has to be adequately addressed.

Currently some insurance companies offer policies covering informational risk. However, the premiums are too high and not affordable to small and medium-sized enterprises.

The following are other reasons why insurers are sceptical about covering informational risk[59]:

- In an ideal world, contract parties' information relevant to the decision is perfect. In an interrelated world, the insurer cannot state with certainty if the insured belongs to a high or low risk class. Unlike him, the applicant knows his level of risk thus creating an information asymmetry between them leading to what is known in economics literature as the **adverse selection problem**.
- Insurers have to contend with the problem of **moral hazards**. These hazards occur when insured firms either intentionally cause a loss or take too few measures to prevent one from occurring. For example, firms may slacken their security if they know they have coverage. The risk of moral hazard requires insurance companies to invest in infrastructure enabling them to observe applicants who need to be reviewed constantly.
- **Internet security externalities** arise from interdependencies that stem from interconnectivity. Computer systems have **interdependent security**, meaning an event on one system may affect all its peers, even if they are under different administrative control. Because of the possibility of aggregating cyber risk exposures, a major concern for insurance companies is single Internet security events causing damage to many policyholders simultaneously.
- Because all risks are not insurable, alternatives must be found when no coverage is possible. Three simple elements of response may be considered to minimize such risks:
- Diminish as much as possible the chance of an incident occurring: (i) by paying particular attention to the relevant preventive measures; (ii) by duplicating data and programs that are not covered (with reliable backup procedures); and (iii) by eliminating as well as possible environmental risks, such as fire and flood;
- Make loss provisions in the accounts;
- Use good practices for infrastructure operation and maintenance (prevention of breakdown).

59 This paragraph was written in collaboration with Igli Tashi.

V.3.4 From data sensitivity to data protection

Analysis of the effective threats and risks, leads to the specification of a security policy that takes into account the protection need of specific resources.

An organization must compile a **resource classification** in order to determine the degree of sensitivity of each of its resources and how important is it to prevent the loss, alteration or disclosure of them. The more serious the consequences for the organization are, the more sensitive (or critical) the resource is; the greater its value and the need to protect it.

For the security or network manager, data sensitivity is important in determining the level of robustness required for systems to protect data and attribute resource access permissions. Users are attributed access permissions as a function of the degree of sensitivity of the data they handle.

The process of determining the degree of sensitivity of data starts with identifying the generic classes of data and their degree of sensitivity. A coherent data classification gives the organization a metric that quantifies the importance of its data.

The following is an example of what the resource classification of one particular enterprise data might look like:

Public	degree of sensitivity - 0
Commercial	degree of sensitivity - 1
Financial	degree of sensitivity - 2
Confidential	degree of sensitivity - 3
Top secret	degree of sensitivity - 4

This classification can be refined according to the specific requirements of specific situations.

Classification of resources can be done with the cooperation of several types of actors as auditors or security and network managers. Each one brings a complementary vision of the problem in order to establish a common view of the *level of criticality* of given data.

The advantage of using auditors is that they are free of the constraints of technical development. This gives them a less biased view of the vulnerability of the organization subsequent to a potential loss, deterioration or disclosure of data. Auditors and administrators may have different perceptions regarding the degree of data sensitivity. If the organization's approach toward assessing data sensitivity is not harmonized, it will likely lead to a proliferation of security measures and restrictions that undermine system performance and prevent users from working in an optimal manner. The organization must find a *judicious compromise* between the conflicting needs of protecting resources and creating a user-friendly cyber-environment. *Too few barriers compromise security, but too many barriers compromise facility of use!*

The network administrator will depend on the security manager to implement logical access control. The existence of quantifiable security metrics that define all users' access authorization will facilitate the process (Figure V.12).

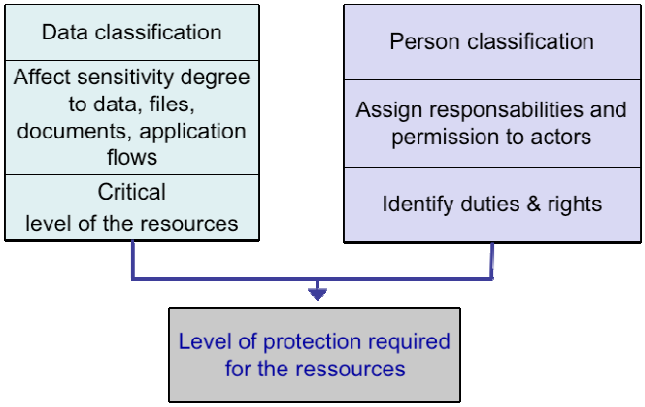

Figure V.12: Classification: a tool facilitating the identification of resources'' protection level

The information security policy determines: (i) the security objectives; and (ii) the measures, procedures, and tools through which those objectives can be reached. In practice, security is implemented incrementally and rarely through a global managerial framework. In many respects, network administrators and technical support are "firemen" treating the most urgent issues by "patch and fix" type interventions. In this context, there is everything to gain from working with products with a security level that can be evaluated or quantified - and to benefit from the security guarantee that those products provide.

V.4 SECURITY ORGANIZATIONAL STRUCTURE

V.4.1 Security organization

An organization's **security structure** should be an *autonomous entity*, independent of operational units and of revision organs. This is called the principle of separation of functions.

The board has the responsibility of approving the security budget. It has the responsibility of ensuring that there is an adequate surveillance management team that will see to it that all employees obey the relevant laws, statutes, regulations and instructions.

The responsibilities of the institutional management are as follows:

- Ratifying the security policy, which contains the philosophy of the security program and the complete set of laws, regulations and practices that govern the manner in which sensitive information is administered, protected and published;
- Designating personnel and assigning their responsibilities;
- Participating actively in awareness campaigns for enterprise employees and managers;
- Presenting the security budget to the board of directors;
- Validating strategic, tactical, and operational plans;
- Etc.

The responsibilities of the security service can be for example as follows:

- Defining the security actions plan (procedure);
- Identifying the security targets;
- Developing and documenting the security policy;
- Creating and maintaining the information and training programs for the staff;

- Identifying, selecting and implementing security procedures, tools and services;
- Organizing and maintaining a crisis management committee and a business continuity plan to make decisions in the event of major disasters;
- Defining the security budget;
- Surveying the development of risks and security requirements;
- Establishing audit programs in collaboration with the auditors;
- Etc.

Depending o organization's size, several high levels managers could be involved in risks and security management as for examples: Chief Executive Officer (CEO); Chief Financial Officer (CFO); Chief Information Officer (CIO); Chief Security Officer (CSO); Chief Information Security Officer (CISO); Chief Legal Officer (CLO); Chief Risk Officer (CRO).

V.4.2 Security audit

In order to establish an effective security program, the various security targets must be subject to an audit. The auditors should be external and mandated by the directors.

The organization needs to have an auditing process in place for each of the following areas. The audits should be carried out within a predefined reference framework:

1. **Financial and Organizational Audit**

- Verification of the suitability of the information technology strategy, program and budget;
- Technical cost analysis;
- Organization and suitability of structures;
- Legal provisions.

2. **Security Audit**

- Verification of physical security;
- Verification of logical security;
- Verification of network security;
- Verification of documentation;
- Verification of insurance coverage;
- Verification of the emergency program (minimal service).

3. **Audit of Operations Centres**

- Analysis of operation, procedures, documentation, organization, system configurations, performance, execution priorities, emergency and recovery procedures.

4. **Audit of Development Centres**

- Verification of internal control and organization;
- Analysis of project management in respect to coordination, development methods, and test data;
- Analysis of quality control.

5. **Audit of Application Reception**

- Analysis of reception procedures and of application maintenance.

6. **Audit of All Actors in the Information System**

- Reliability of equipment, availability of resources, operational modes, etc.

Security administrators are persons in contact with the security targets (resources to be protected). They have the responsibility of maintaining operational condition. They mainly carry out the following tasks:

- Management and administration of security means and measures necessary for the target they are responsible for;
- Definition of access privileges in a manner that does not permit end users to access or interfere with the resources of other users;
- Re-evaluation of access privileges on a regular basis;
- Elaboration and maintenance of administrator and user documentation;
- Supervision of the security target through the analysis of all incidents compromising security and definition of actions required to resolve them.

In the context of security management, human resources managers have the following responsibilities when recruiting new staff, as for example:

- Check necessary information before the recruitment;
- Inform new recruits of their responsibilities in the security domain; transmit them the security directives and their first passwords;
- Ensure that new employees sign professional secret declarations stating they will not reproduce sensitive information, and that they will adhere to the security policy;
- Coordinate, with the security manager, particular actions having to be carried out at the end of every work contract.

Department heads have the following responsibilities:

- Ensure that their staff and consultants are informed about the security policy so they can respect its directives;
- Inform the relevant security administrators of all modifications having a potential impact on the level of security or its management;
- Analyze, validate and take position on resource access requests presented by their staff;
- Inventory sensitive information held by members of the team and recover it when they leave the company.

Information systems' users have to:

- Respect the rules and practices defined by the security policy;
- Keep the enterprise's confidential information secret;
- Use the enterprise information technology resources made available to them only for professional ends;
- Inform the security administrator of any element having a potential impact on security.

An organization must have a coherent business security *ethic* including an ICT security ethic that is adopted by all the actors. This ethic should be laid down in a *charter* that is recognized and honored by all. It is not sufficient for all involved to sign a security charter; they must also be able to respect it. A professional code of ethics governing the use of data processing and Internet resources must include items related to:

- The field of application of the charter;
- Access to data-processing resources and services;

- The rules for a professional, rational and honest use of the resources;
- The security procedures;
- Confidentiality limitation;
- Appropriate information technology legislation.

An organization often needs extensive training and dissemination of information on the stakes, risks and preventive measures relating to security, in order to educate its entire workforce on its security approach. The organization should also publicize its application of dissuasive measures as well as penal consequences resulting from non-compliance with security obligations.

V.4.3 Protection against intrusion and reaction to malicious incidents

When possible, it is imperative to prevent incidents by putting in place appropriate protection measures (access control, insulation, filtering, etc.) and when not, to detect them (monitoring) in order to react quickly and limit the damage while optimizing the chances of identifying the intruders (reaction).

An organization should have clear, precise and comprehensible directives that specify what the person in charge of security or the system administrator should do in the event of a disaster. Disaster recovery occurs in a context of emergency and is always a critical situation. It is of primary importance to help security people to control the situation. Planned backup, recovery and notification measures will facilitate decision-making and avoid a state of panic that is prejudicial to the maintenance of security.

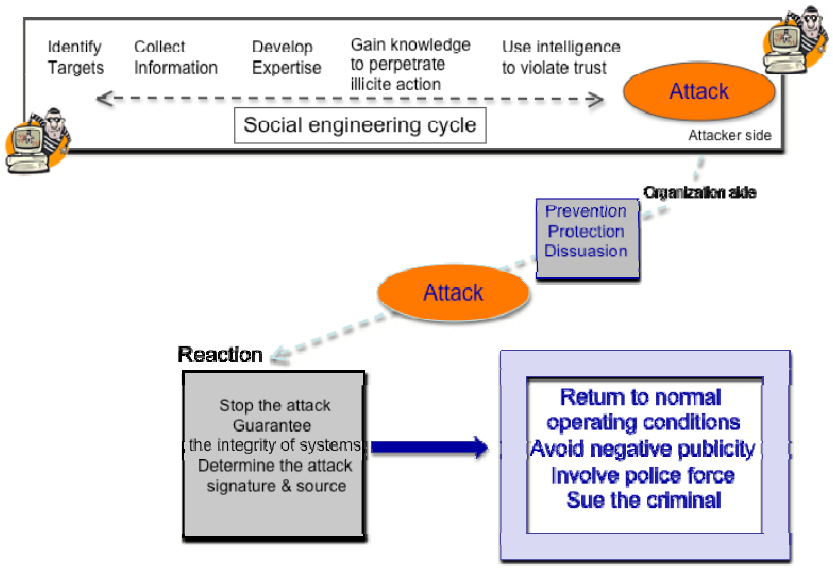

Figure V.13: Reaction to an attack

Figure V.13 presents a cyberattack reaction plan. It includes:

- Preventive measures, such as the controlling, monitoring, and safeguarding of vital data, and active audits;
- Measures of dissuasion, such as notification of the recording of actions and events, and complaints lodged with the police force;
- Structural measures (organization and responsibility);

- Protection measures, such as certification, access control procedures, cryptography, proof of origin, filtering, and isolation of digital environments;
- Measures of report and notification, such as recording malicious acts, reporting and verifying the infringement, and notifying management and victims;
- Recovery measures, such as help, safeguards, restitution, and return to normal;
- Legal measures to bring the intruder to justice.

A **prevention strategy** consists of setting up appropriate security measures and monitoring the overall computer and network activities. The log of events and their analysis can facilitate the identification of abnormal situations leading to potential security problems.

Several **attack recognition** software programs - called **Intrusion or Incident Detection Systems (IDS) -** are available. They function in a very similar way to anti-virus software. They identify attacks according to a certain signature, which is called an **attack pattern**. The development of new types of attacks implies that it is vital to constantly upgrade incident detection systems.

Some of these programs follow attack recognition methods based on predictable user behavior. This is called derivation of normal procedure. Their efficacy depends especially on their capacity to correctly distinguish normal activities from those leading to intrusions. Once a system has detected a suspicious event, it should be capable of recording it, generating a report, and alarming the users to activate security mechanisms or to end connections in progress. Warning may be sent by electronic messages or by pager alerts to operators.

Identifying the phase of intelligence gathering is important in order to prevent an attack from being carried out. A strategy of attack recognition will be more effective if the person in charge of security knows the strengths and the weaknesses of the established security measures. Human resources management adapted to security needs is an important component for internal risk prevention. The security administrator should have an idea of how attractive a given system is to potential criminals. Higher attractiveness leads to higher attack risks.

A **reaction strategy** involves five types of action:

- Identification of the attack;
- Evaluation of the goal of the attack (vandalism, diversion, etc.);
- Alert, report and notification (legal service, etc.);
- Blocking the attack;
- Recovery and return to normal situation as rapidly as possible.

To prevent threats, an organization must have in-depth knowledge of the environment to be protected and of the values to be preserved. An elementary rule is to avoid the attribution of excessive privileges to users when systems are configured, even if it means increasing user's rights gradually according to need, and then, only for a limited duration.

The following steps increase the security level of an organization: (i) warning users about security problems; (ii) obtaining users promise to use the information technology resources only for professional means; and (iii) implementing authentication procedures, non-permissive configurations, and monitoring mechanisms.

V.4.4 Defining a Disaster Recovery Program

A **Business Continuity Plan (BCP)**[60] contains different procedures and time scales for different levels of failure. In the aftermath of an incident, a BPC incorporates emergency procedures to ensure the safety of all affected staff members, and covers the planning and procedures to resume normal

60 This paragraph was written in collaboration with Igli Tashi.

operations upon recovery. It includes procedures for re-establishing the telecommunications and network services used by the organization.

An **emergency program** is a technical and organizational structure that makes it possible to ensure a minimum service of critical applications after a disaster. It should do the following:

- Define a recovery strategy;
- Identify the minimum time lapse between an incident and recovery - this is the concept of critical delay;
- Identify the events and actions required to make a successful recovery - these include synchronization, distribution of actions, insurance declaration, and identification of exceptional costs.

An emergency program is made up of several sub-programs, as shown in Figure V.14.

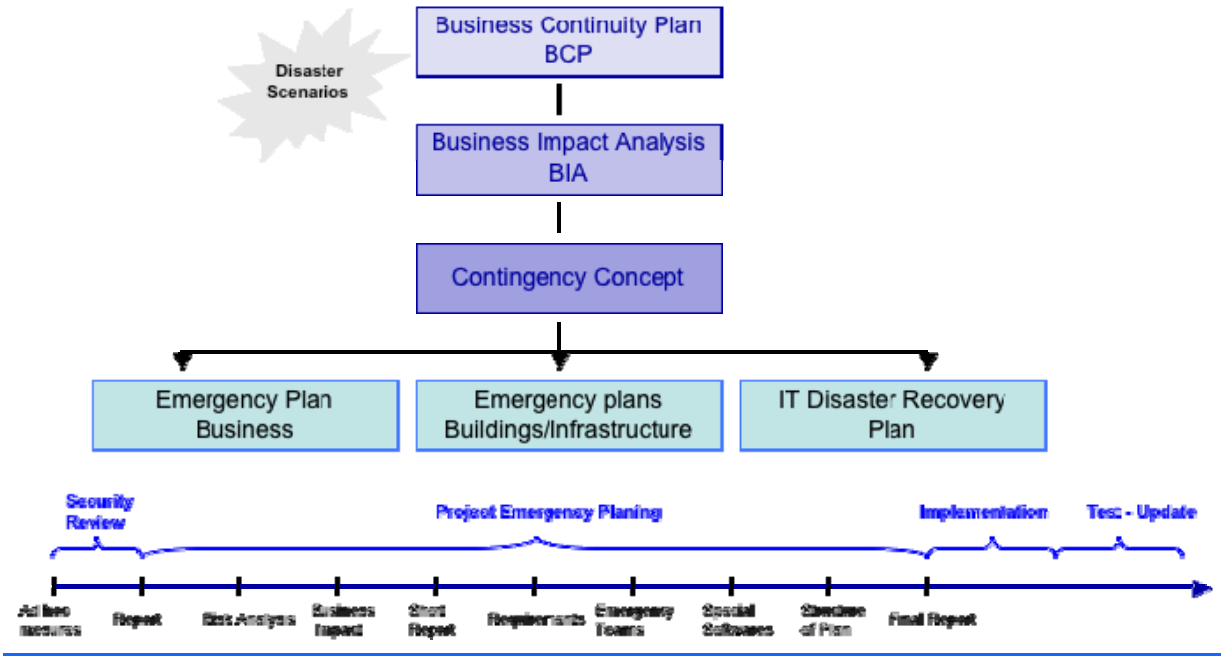

Figure V.14: Structure of a business continuity plan and disaster recovery plan

An organization should integrate its *emergency plan* into a project management approach. A **design methodology** ensures that the steps of an emergency plan are carried out in a well-controlled and systematic manner.

The **strategic analysis** step is built around four principal tasks (Figure IV.15):

1. **Project Organization and Management**: Identifying a team and an organizational structure; The project leader should have centralized responsibility, an enlarged visibility and appropriate authority; Planning - coordination and organization of the implementation and update of the emergency program; Training and assistance of persons working on the security program;
2. **Risk Analysis**: Risk evaluation and definition of potential disasters;
3. **Impact Analysis**: Definition of fragility criteria and risk sensitivity of applications; Analysis of different breakdown, error and malfunction consequences; Evaluation of strategic and tactical impacts;

4. **Definition of Normal and Minimum Service Levels** for each critical application: Definition of maximum inactivity delay, operational instructions, restore priorities for critical applications, recovery procedures; Identification of planning requirements.

After strategic analysis, the next step is **operational implementation**. This consists of **solution analysis** to identify, evaluate and select the most appropriate solution in light of the strategic criteria.

Rendering the emergency program operational requires: (i) assigning responsibilities; (ii) informing and training responsible persons in the execution of recovery procedures; and (iii) maintaining full documentation of the emergency program.

Next is the **validation** step. This implies testing the program and its efficiency by simulating alerts and documenting and analyzing the results. Part of its operational management is updating changes in personnel and modification applications on a day-to-day basis.

The objective of the **emergency program audit** is to determine the established program's quality. First, the audit identifies the sensitive areas of the organization. Next, it evaluates the program's provisions, procedures, tasks and actions for coping with an incident. Then, it makes recommendations.

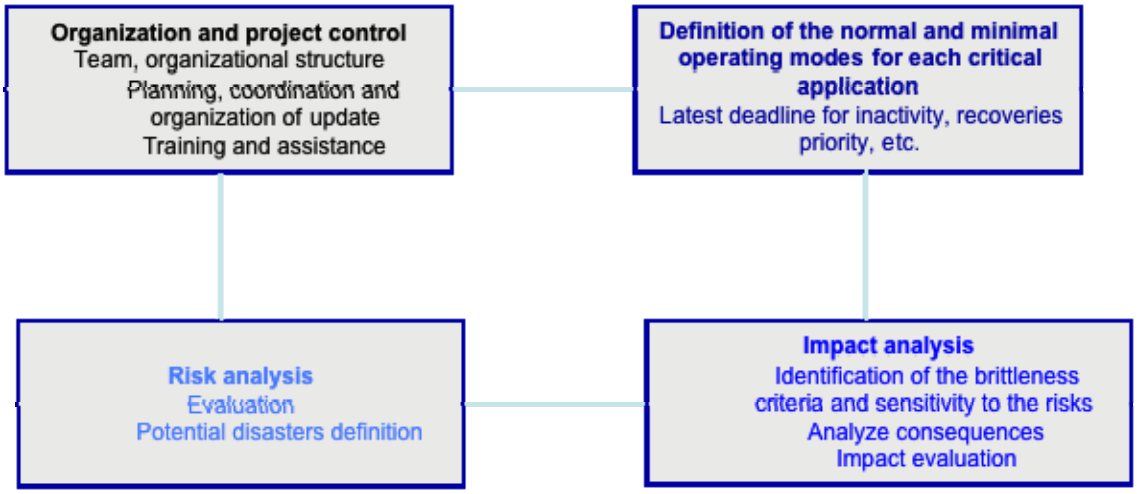

Figure V.15: Design methodology of a disaster recovery plan (strategic analysis step)

V.5 SOME BASIC RECOMMENDATIONS TO IMPROVE CYBERSECURITY EFFECTIVENESS

The following points should be kept in mind when dealing with cybersecurity issues:

- Security is everybody's business.
- Too much security is as much a problem as not enough security.
- The hardest thing is not deciding which technology to implement, but rather identifying why it should be implemented and on what.
- Security should be a function of risk and in proportion to the stakes.
- Security is never definitively acquired and should be lived out on a day-to-day basis.
- The quality of security tools depends on the security policies they serve.

- A security policy should not be designed on the basis of the limitations of specific systems (operating systems, applications software, etc.).
- The greater the reward, the greater the risk of penetration of a system (notion of attractiveness of an organization as a target);
- Adopt a business and ICT security ethic.

ANNEXES

I. Annexe A – Glossary of main cybercrime and cybersecurity related terms

- A -

Access control
Mechanism that serves to protect a resource (a service, system, data or program) from inappropriate or unauthorized use.

Accident
Unforeseeable incident causing prejudice to an entity.

Active attack
Attack which alters the targeted resources (affecting integrity, availability, confidentiality).

Adware
Adware, meaning advertising supported software, is a piece of software bundled with a program. It is designed to automatically download or display advertising banners as soon as the computer user installs the program. An adware is different from a spyware in the sense that an adware does not aim to collect private information in order to perform theft. But a controversy still takes place with adware, as some adware actually gathers information about the user in order to send more personalized advertisement.

Anomaly detection
Anomaly detection analyses a set of characteristics of the system and compares their behaviour with a set of expected values. It reports when the computed statistics do not match the expected measurements.

Anonymity
Characteristic of an entity whose name is unknown or which does not reveal its name, allowing an entity to use resources without being identified (incognito). Provision should be made to respect the wish of certain users who may have a valid reason for not revealing their identity when making statements on the Internet, in order to avoid excessive restriction of their freedom of expression, to promote the free expression of ideas and information and ensure protection against unauthorized online surveillance by public and private entities. On the other hand, judicial and police authorities should be able to obtain information on individuals responsible for illegal activities, within the limits set by national law, the European Convention on Human Rights and other international treaties such as the Convention on Cybercrime.

Antivirus
Program designed to detect a kind of malevolent code (virus).

Asset
Something that has a price and which represents a form of capital for its owner (concept of sensitive asset). In terms of security it is important to determine assets and to classify them by degrees of importance, in order to implement the requisite adequate measures of protection and thereby avoid losing them or at least minimize the adverse impact of their loss.

Asymmetric cryptographic algorithm
Algorithm based on use of a pair of keys (one for data encryption and the other for decryption).

Attack
Assault, aggression or action causing prejudice to individuals or resources. There are different types of computer−related attacks.

Attacks against critical infrastructure
An attack targeting specific vital infrastructures such as electric power supplies, nuclear power facilities, water supply schemes, etc.

Attack tool
An attack tool is an automated script (program) designed to violate a security policy.

Auditability
The extent to which an environment lends itself to being analysed for the purposes of analysis and audit.

Auditing
Auditing is the analysis of log records to evaluate and to present information about systems in a clear and understandable manner. Most often it is done for optimization or validation purpose.
The conduct of an independent review and examination of system records and activities.

Auditor
Person conducting an audit.

Authentication
The act of authenticating. Authentication serves to confirm (or refute) that an action, a declaration, an item of information is authentic (original, genuine). Process used in particular to verify the identity of an entity and to ensure that it matches the previously recorded identity of that entity.

Authenticity
The character of that which is authentic. The characteristic allowing for attestation, or certification of validity. Often associated with the fact that an item of information or an event has not been altered, modified or falsified and that it was indeed produced by the entity claiming to have originated it.

Authority
A body with the power to exercise prescribed functions. Generally used to refer to a body in charge of issuing digital certificates.

Authorization
The act of authorizing, allowing, entitling. Permission to carry out certain actions, grant rights, obtain right of access to a service, information, a system, etc.

Availability
Security criterion whereby resources are available and usable in order to meet requirements (no denial of authorized access to systems, services, data, infrastructure, etc.).

- B -

Backdoor, trapdoor
Usually refers to a portion of code incorporated into software that allows unauthorized entities to take control of systems, copy information, etc., without the owner’s knowledge.
Any undocumented access point into an otherwise secure computer system. Back doors are most often created by software developers in the case they would need unfettered access to a system for repair. These entry points present serious risks when accessed by outside intruders because they are less

heavily protected than normal access routes. They are also a point of concern because they are usually hidden from anyone except from the original developer, who may retain access privileges even after termination from the company.

Bacterium
Kind of malicious software that multiplies so rapidly that resource become exhausted, thus creating a denial of service attack. A program that entirely absorbs some classes of resources is called a bacterium or a rabbit.
A type of malware that creates many instances of themselves or run many times simultaneously, in order to consume large amounts of system resources. This creates a denial of service effect as legitimate programs may no longer be able to run, or at least may not run properly.

Backup plan
The set of technical and operational means foreseen to ensure the sustainability of information and the continuity of activities, no matter what the problems encountered.

Back up
A copy of a program or data file for the purposes of protecting against data losses if the original becomes unavailable.

Behavioural evidence
Any type of forensic evidence that is representative or suggestive for a given behaviour.

Behaviour evidence analysis
The process of examining forensic evidence, victimology and crime scene characteristics for behavioural convergences before rendering a deductive criminal profile.

Business continuity management
A management process that identifies potential risks and their impacts on the institution and provides a framework for building resilience and capabilities to respond to these risks, hence to reduce their impact on the organization’s reputation, image and value created activities.

Bot
Bots are programs, generally executable file installed on a computer in order to run a set of functions automatically and allow an illegitimate user to gain remote control through a communication channel.

Botnet
Bots never work alone; they are part of a big network of infected computers (or *zombies*), called botnet (standing for bots network). In every bot, a back door has been installed to be able to listen to commands. An IRC channel or Peer-to-Peer network allows the cybercriminal to centrally control the zombies and to launch coordinated and simultaneous attacks.

Breach
Effect of or deterioration resulting from an act of aggression or attack whose impact may be: tangible (physical or material alteration, logic malfunction, disorganization of procedures, etc.); logical (non-availability, loss of integrity, breach of confidentiality); strategic (in particular as concerns finance, additional costs for hosting, transportation, telecommunications, expertise, purchase/rental of hardware and software, personnel, outsourcing, operating losses (profit margin, cash flow, customer losses), loss of funds or goods, etc.).

Buffer overflow
A buffer is a temporary data storage area with a limited storage capacity. A buffer overflow occurs when a program tries to store more data in a buffer than the storage capacity. The data will overflow into another buffer, and thus overwrite and corrupt the data stored in these adjacent buffers. Hackers often launch buffer overflow attacks with extra data that contain specific instructions to corrupt the

system or to send instructions to the targeted computer, in order to damage, change or gather confidential information.

Bug
Fault in machine, computer system or program.
A programming error. By analogy, a conceptual or implementation defect that is revealed by malfunctions.
Bogus email and/or website are bugs intended to induce victims to voluntary disclose information.

Byzantine failure
A Byzantine failure refers to misbehaviour, malfunctioning of a system or network. It could have a malicious origin.

- C -

Certificate, public-key certificate
The set of data issued by a certification authority (trusted third party) and used to provide security services (confidentiality, authentication, integrity). A digital certificate uses public-key encryption. The certificate includes the value of the subject's public key, attested by the fact that the certificate is signed by the issuing certification authority.

Certification Authority (CA)
Trusted third party for the establishment, signature and publication of public-key certificates.

Chief security officer (CSO)
The person in charge of the security of information technology systems.

Cipher
Encryption algorithm used to transform plain text into ciphertext.

Ciphertext – see *Cryptogram.*

Compliance
Conformity, agreement with; compliance with standards.

Computer crime
The mean or the target of an illicit action is a computer (theft of computer services, unauthorized access, software piracy, theft of digital information, extortion committed with the assistance of computers, …).

Computer forensics
Computer forensic consists of computer investigation and analysis to examine, identify, collect and preserve digital evidence. It is the act of looking for and preserving digital evidence of a crime for eventual uses in Court. This process often involves the investigation of computer systems to determine whether they are or have been utilized for illegal or unauthorized activities. Computer forensics experts identify sources of documents or other digital evidence; preserve and analyze the evidence and present the findings.

Computer virus
A computer virus is a program that inserts itself into one or more files and then performs some kind of malicious action.
A boot sector infector is a virus that inserts itself into the boot sector of a disk.
A multipartite virus is one of a kind that can infect either boot sectors or applications.
A terminate and stay resident (TSR) virus stays active (resident) in memory after the application (or bootstrapping, or disk mounting) has terminated.
A stealth virus is a virus that conceals the infection of files.

An encrypted virus enciphers all virus codes except a small decryption routine.
A polymorphic virus is a virus that changes forms each time it inserts itself into another program.
A macro virus is a virus composed of a sequence of instructions that are interpreted, rather that executed directly.

Computer worm
A computer worm is a variant of a virus, it is a program that copies itself from a computer to another.

Confidentiality
Keeping information and transactions secret. The nature of that which is secret. A security objective aimed at preventing the disclosure of information to unauthorized third parties and at protecting that information from reading, eavesdropping and illicit copying, whether accidental or deliberate, while it is being stored, processed or transported (concept of data confidentiality).

Contingency Plan
Documented organized process for implementing emergency responses, back-up operations and post-disaster recoveries, being maintained for a management information system as part of its security program to ensure the availability of critical assets (resources) and facilitate the continuity of operations in case of emergency.

Continuity Plan
Plan by which information technologies and telecommunication capabilities are recovered and restored following the occurrence of a significant emergency, incident, crisis or event.

Control Objectives for Information and related Technology (COBIT)
Control Objectives for Information and related Technology is a set of IT governance and security guidelines that were first published in 1996. COBIT, issued by the IT Governance Institute, is gaining by day an increased international acceptance amongst IT specialists and accepted as good practice for information control, IT and related risks.

Cookies
Piece of program written to Internet users' hard disk without their knowledge, when they access certain websites, and that collect data on the users' web behaviour, in principle, to customizing the web services offered.

Copyright
A copyright is a type of intellectual property consisting of a set of exclusive rights that limits and regulates the use of a protected content.

Corpus delicti
Refers to essential facts that show a crime has taken place (body to the crime).
A term from jurisprudence that refers to the principle in which it must be proven that a crime has occurred before a person can be convicted of having committed a crime.

Countermeasure
System security function, measure, procedure or mechanism aimed at reducing the level of vulnerability and at countering a threat before it becomes a reality.

Cracker
A person who breaks the copy protection of a software.
An individual who breaks into computers much like a safecracker would break into safes.
A person who enters a computer system without permission. Motivations behind the trespassing action may be malicious or based on curiosity. Some altruistic crackers might be willing to notify the system administrator of vulnerabilities they discover.
A program that could detect weak passwords or break them.

Crime
Activities that involves breaking the law. An illegal act or activity that can be punished by law.

Crime reconstruction
Determination of actions surrounding crime commitment. This may be done by utilizing the statements of witnesses, suspect confessions, statements of living victims or by examination and interpretation of physical evidence. (Some refer to this process as crime scene reconstruction, when only actions are being reconstructed)

Crime scene
A location where a criminal act took place.

Crime scene characteristics
The discrete physical and behavioral features of a crime scene.

Crime scene type
The nature of relationship between offenders' behaviour and the crime scene in the context of an entire criminal event.

Cryptanalysis
The set of methods used to analyse previously encrypted information in order to decrypt it; cryptanalysis is therefore also referred to as "decoding". The more robust the encryption system, the more difficult cryptanalysis becomes.

Cryptogram, **ciphertext**
Data that have been cryptographically transformed. Encrypted data, text or message. Data obtained by encryption.

Cryptographic algorithm
Algorithm used for data encryption in order to make the data confidential; it is based on a mathematical function and an encryption key.

Cryptographic period
Period of time during which a system's keys are not changed.

Cryptography
The mathematical application used to write information in such as a way as to render it unintelligible to those who do not have the means of decrypting it. See *Encryption*.

Cybercrime
A computer system is the mean or the target of a crime committed using Internet technologies.

Cyberinsurance
Cyberinsurance covers a number of areas not usually spelled out in traditional policies. These areas include denial-of-service attacks that bring down e-commerce sites, electronic theft of sensitive information, virus-related damage, losses associated with internal networks crippled by hackers or rogue employees, privacy-related suits, and legal issues associated with websites, such as copyright and trademark violations.

Cyberspace
The place created trough the interconnection of computer systems by the Internet.

Cybersquatting
Act of registering a popular domain name address for the purpose of reselling it later to its rightful trademark owner in order to acquire profits. Cybersquatting can be considered as extortion.

Cyberstalking
The use of computer networks for stalking and harassment behaviours. Many offenders combine their online activities with more traditional forms of stalking and harassment (telephoning the victims for example).

Cyberterrorism
A kind of terrorism utilizing cyberspace and ICT resources to attack critical infrastructures or to optimize classical terrorism activities.

Cybertrail
Any digital data left by a victim or an offender into systems and networks in order to lead to some identification (of a place, of an individual, of an action, etc.).

- D -

DDoS (Distributed Denial of Service)
A saturation (or denial of service) attack launched from several systems simultaneously.
A distributed denial of service attack uses a large number of computers infected by a worm or a Trojan horse to launch simultaneous attacks at a target in a very short time. For example, Zombie computers can bombard a system with thousand of emails causing a denial of service at the Mail server and thus denying service to legitimate users. The continuous growth of bot networks and their increasingly better coordination can explain the rise in DoS attacks.

Deviance
Variation from a normal to an abnormal behaviour.

Demilitarized zone (DMZ)
The DMZ is a portion of a network that separates a purely internal network from an external network such as Internet.

Digest
The string of characters formed when a hash cryptographic function is applied to a series of data.

Digital evidence
Any digital data that can establish that a crime as been committed or that can provide an alibi or a link between a crime and its victim or a crime and its perpetrator.
Any information of probative value that is either stored or transmitted in digital form.

Digital investigator/digital crime scene technician
Individual responsible for data searching and gathering at a computer related crime scene.

Digital signature
By analogy to a handwritten signature, the digital signature obtained via an asymmetric encryption algorithm is used to authenticate the sender of a message and to ascertain the message's integrity.

Direct losses
Identifiable losses resulting directly from a security defect.

Dissuasion
Means used to deter malicious attackers from carrying out an attack, by persuading them that what they stand to gain is negligible in comparison to the losses that the system they threaten to attack could inflict.

DoS (Denial of Dervice)
A denial of service attack consist in sending a large number of packets in large bursts to a system (*packetting*) and in order to flood it. The system will not be operational anymore.
A type of network attack that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being created.
A denial of service attack aims to prevent legitimate users from accessing a site or a service by limiting the target ability to service legitimate requests. Generally, DoS attacks aim at consuming all target resources in order to saturate the Internet connection. DoS tools are designed to send many request packets to a targeted Internet server (usually Web, FTP, or Mail server) in order to flood the servers' resources, thus making the system unusable. Any system or computer connected to the Internet is vulnerable to DoS attacks.

- E -

Eavesdropping
This term originally referred to simply listening to a conversation, but now it has taken on digital implications. The interception of e-mail, SMS, voicemail or facsimiles now falls under eavesdropping. This type of data collection can present an easier way of obtaining relevant passwords and authentication keys without needing to enter into a secure system.

Efficiency
The quality of doing something well with no waste of time or money.
The quality of that which has the anticipated effect, which produces useful results. Characteristic of security measures that are relevant and have a genuine capacity to protect a resource, with a minimum of investent.

E-mail Bomb
A piece of malicious code that, when activated, sends a large amount of e-mail messages to one address in order to overload and potentially freeze an e-mail server or fill disk space.

Emergency plan
The set of technical and organizational means foreseen to respond optimally to a serious incident that is harmful to the organization and affects the smooth conduct of operations.

Encryption
The cryptographic transformation of data (cryptogram) to guarantee confidentiality. Encryption consists in making data incomprehensible to anyone who does not have the decryption key. Plain text is encrypted using an algorithm and an encryption key in order to create ciphertext, which can be decrypted using the corresponding decryption key (except in cases where the encryption is irreversible). The inverse operation is called decryption, or decipherment.

Ethic
Moral principles that control or influence a persons' behaviour.
The principles of right conduct with reference to a specific profession, mode of life, etc. (code of ethic).
Moral value systems are systems of principles governing morality and acceptable conducts.
Ethics is the branch of philosophy that deals with moral principles.

Exposure
An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either: allows an attacker to conduct information gathering activities; allows an attacker to hide activities; includes a capability that behaves as expected, but can be easily compromized; is a primary

point of entry that an attacker may attempt to use in order to gain access to the system or data; is considered a problem according to some reasonable security policies.

- F -

Failure
Malfunction, breakdown making the resource unavailable.

Firewall
A firewall is a system that mediates access to a network, allowing or disallowing certain types of access on the basis of security policy rules. A filtering firewall performs access control on the basis of attributes of headers of IP packets analysis (source, destination addresses).

Flaming
Technique that consists of sending large numbers of inappropriate messages in order to undermine the credibility of a discussion group.

Flooder
A malicious program utilized to slow down communications between the access provider and the Internet user, or to disconnect the user.

Frauds
Wilful deceit; trickery as: blackmail, illegal downloading of software, music, movies (piracy), online fraud: Internet auctions, advanced fee frauds, Internet fraud actions. (Internet auction sites can be used by thieves to access an international market to sell stolen items (Internet as a market for stolen goods). Nigerian letter/Scam: A typical letter claims to come from a person needing to transfer large sums of money out of the country. As the Nigerian letter variation of fraud has become well known, the gangs operating the scams have developed variations to that. The target is often being told that they are the beneficiary of an inheritance or are invited to impersonate a beneficiary of an unclaimed estate.
Telemarketing fraud: Telemarketing fraud is a term that generally refers to any defraud scheme in which the persons carrying out the scheme use the telephone as their primary means of communication with prospective victims and try to persuade them to send money to the scheme.

Fraudster
A person who practices fraud.

- G -

Guest account
An account that does not have a specific, individual User ID associated but rather a more generic ID such as “guest”. Such accounts are generally intended for temporary use by authorized visitors, they must be kept to a minimum and must be restricted to captive accounts.

Guideline
A guideline is typically a collection of system specific or procedural specific “suggestions” for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

- H -

Hack
The act of entering a system illicitly.

Hacker
A person who, for whatever reason, enters someone else’s system without authorization and unlawfully. The attack may be passive or active.

Hacking
The series of operations used to breach an information technology system.

Hacktivism
Political activism and social protest that uses hacking tools and techniques.

Hash function
In the context of encryption, this is also referred to as the digest function. Starting from the message data, it generates a message digest, i.e. a kind of digital fingerprint, which is shorter than the original message and incomprehensible. This is then encrypted with the sender's private key and attached to the message to be transmitted. On receipt of the message and its fingerprint, the recipient decrypts the fingerprint with the sender's public key, recalculates the fingerprint from the message received using the same hash function, and compares it with the fingerprint received. If the result is the same, the recipient has thus verified the sender's identity and is assured of the message's integrity, since, if the message is altered, even only slightly, its fingerprint is significantly modified and the message has been deleted.

Hidden crime
Criminals' acts that tend to go largely unobserved, unnoticed and unrecorded in official assessments and measures of criminal activity.

High risk transaction
A none secured transaction (or its security is out of date) that is performed in a hostile environment.

Hijacking
Hijacking means taking control of an established communication between two entities.
Two major forms of hijacking are browser hijacking and TCP session hijacking. Browser hijacking consists of the redirection of the user to a different website than the one he requested. The attacker can perform this attack by accessing the DNS records stored on the server and modifies them by changing the expected webpage into the fake webpage. The TCP session hijacking is an attack on a user session. The attacker seizes control of the communication between two legitimate nodes by inserting commands or fraudulent traffic into the data stream and by disguising himself he becomes a legitimate and authenticated user.

Honeypot
An unpatched, default system whose goal is to attract and log the probes and attacks of malicious hackers and crackers. These traps primarily aid in data collection and do not offer any direct protection to a network. Honeypots can be used to glean data about illegal activities and analyze potential system weaknesses. Honeypots can also provide an environment for post-attack forensic analysis.

- I -

Indecency
Behaviour that is thought to be morally offensive.

Identification
The process by which one can recognize a previously identified entity.

Identity
Information used to designate and distinguish, if possible in a unique and unambiguous fashion, a specific entity within a naming domain.

Identity theft
A crime in which a fraudster illegally obtains confidential and personal information, such as credit card number, social security numbers, passwords or banking account numbers in order to impersonate the victim. Once the criminal is in possession of these credentials, he can either access the victims'

account, perform withdrawals, purchases or open new accounts such as credit card accounts or cell phone accounts, by using the stolen identity. In order to steal this information, the attacker might break into the system or lure its victim with phishing attacks.

Impact
Expresses the level of consequences produced by an attack (**financial impact**: cost of the attack; **logic impact**: undermines availability, integrity, confidentiality; **strategic impact:** detrimental to the organization's survival; **tangible impact**: a real, directly observable effect).

Impact gravity
Assessment of the seriousness of an incident, weighted by its frequency of occurrence. It is important to quantify impact gravity in order to pinpoint and prioritize security requirements, for example: no/negligible impact (0), little impact (1), moderate impact (2), strong impact (3), disastrous impact (4).

Imputability
The quality that makes it possible to impute an operation to a user at a given time with certainty. The fact of being able to identify who is to be held accountable in the event of a violation of the rules.

Indirect losses
Losses generated indirectly by a security defect.

Information dominance
The act of controlling information.

Information security risk assessment
A calculation of the probability of loss or injury based on possible threats to existing or future infrastructure. The organizational impact of these threats should be carefully assessed before introducing information safeguarding measures.

Information system
Information and communication infrastructures and resources (computer, network, data, program, etc.) belonging to an organization, organized and managed in order to contribute to realize the organization strategy.

Information warfare
The activity of competing in aggressive ways with another group, company, etc. using information "as weapon".

Insider
A person who knows about the internal working manner of an organization.

Intangible goods
Goods owned by organizations but impossible to be perceived by the senses (digital information).

Integrity
The state of something that has remained intact. Security criterion which, if met, makes it possible to ensure that a resource has not been altered (modified or destroyed) in unauthorized fashion.

Intellectual property
Property that derives from the work of an individual's mind or intellect.
Early copyright law aimed to protect the economic interests of book publishers rather than the intellectual rights of authors. Modern copyright law protects the labour of elaborating an idea, but not the idea itself. The concept of discovery also plays a role in intellectual property rights: a patent is awarded to one who can demonstrate that he or she has invented something not previously known.

In law, property is something that is owned or possessed. Concepts of property vary widely among cultures.

Internet
Publicly accessible computer network connecting many networks from around the world for the purpose of exchanging data electronically. Internet is a network of networks.

Intranet
An organization's internal, private network using internet technology and usually insulated from the internet by firewalls.

Intrusion detection system (IDS)
System for detecting incidents that could result in violations of security policy and diagnosing potential breaches.

IPSec (Internet Protocol Security)
A version of the Internet Protocol that offers security services. IPSec opens a logical communication channel (IP tunnel) between two correspondents on the public internet. The tunnel ends are authenticated and the data transported through them can be encrypted (concept of encrypted channel or virtual network).

IPv6 (Internet Protocol version 6)
Update of IPv4, incorporating, *inter alia*, built−in mechanisms for implementing security services (authentication of source and destination entities, confidentiality of transported data).

IRC (Internet Relay Chat)
Internet Relay Chat is a form of real-time conversation through the Internet (synchronous messaging system conferencing). Group communications as one-to-one communication are possible.
IRC are designed to enable Internet users to join online discussion in forums, called channels. IRC is not limited to just two participants. IRC are commonly used by criminals to exchange ideas, attack's tools or to send command to zombies and launch large attacks. IRC forums could be also a meeting place for criminals.

ISO 17799, ISO 2700x
Information security management standards set by the International Organization for Standardization.

- J -

Jurisdiction
The right of a Court to make decisions regarding a specific person (personal jurisdiction) or a certain matter (subject matter jurisdiction).

- K -

Key
Encryption or decryption logical key of an encryption algorithm. Unless they are public, encryption keys should not be disclosed: they are a secret means of protecting another secret (the information that was encrypted in order to ensure its confidentiality).

Keylogger
Keylogger is a program that monitors the keys typed by the user and then either stores the gathered information on the computer or directly sends it back to a server. It is often through a Trojan horse, a virus or a worm that a keylogger is installed on a computer. For example, one Trojan horse activates the keylogger as soon as some specific words like "credit card", "account" and "social security number" appear in a browser. The malicious program will then record everything that has been typed by the user during a legitimate transaction and will send the recorded information to the cybercriminal.

Keystroke-logging
Keystroke-logging utility is a diagnostic tool used in software development that captures the user's keystrokes. It can be useful to determine sources of error in computer systems and it is sometimes used to measure employees' productivity on certain clerical tasks.

Key management
Management of encryption keys; generation, distribution, archiving, destruction of keys in keeping with security policy.

- L -

Logic bomb
A malicious program triggered by a specific event such as a birthday date and intended to harm the system in which it is lodged. A logic bomb is a program that performs an action that violates a security policy when some external event occurs.

Logging
Logging is the recording of events or statistics to provide information about system use and performance.

Loss of essential service
Total or partial unavailability or malfunction of the resources required for a system or organization to operate properly.

Low risk victim
An individual whose personal, professional, and social life does not normally expose him to a possibility of suffering harm or loss.

- M -

Malevolent
Said of hostile actions liable to harm an organization's resources, which may be committed directly or indirectly by people inside or outside the organization (theft of hardware, data, disclosure of confidential information, illicit breaches, etc.).

Malware– malicious software
A generic term for a program such as a virus, worm or Trojan horse, or any other form of attack software that acts more or less independently.

Man in the middle attack (MiM)
A man-in-the-middle attack is an attack in which an attacker is able to read, insert and modify at will, information transferred between two parties, without either party knowing that the link between them has been compromised.

Masquerade
Type of attack based on system decoy.

Method of approach
Offenders' strategy for getting close to a victim.

Modus operandi (MO)
"A method of operating" that refers to the behaviours that are committed by an offender to realize an offence.

Monitoring
The action of watching and checking something carefully for a period of time to discover information about it.

Multi-factor authentication
Multiple proof of users' identity when accessing a system (password, biometry, etc.).

- N -

Non-repudiation
The capacity to prevent a sender from subsequently denying having sent a message or performed an action. Guarantees the availability of evidence that can be submitted to a third party and used to prove that an event or action occurred. Evidence that a message was sent by a specific person at a given time, without having been subsequently modified. Such evidence should be verifiable by a third party at any time. Without non-repudiation, information senders and recipients could deny that they received or sent the information in question.

No-opt
Service in which the customers cannot choose how the information on them is used (possibility that their right to data privacy will be infringed).

Notarization
Registration of data for the purposes of evidence.

- O -

One-way hash function
A function that can be used to calculate the data fingerprint, but not to generate data that have a specific fingerprint. This function must avoid producing collisions, i.e. the same profile being generated from different messages.

- P -

Packet sniffing
Attack, which consists of using a sniffer in order to intercept the traffic over a network.

Passive attack
Attack which does not alter a target (passive listening, breach of confidentiality).

Password
Confidential information to be produced by an authorized user in order to prove his identity during the authentication procedure for requesting access to a resource.

Patch
A software update aimed at repairing a weak spot identified after the software was installed.

Penetration tests
These are used to analyse and test the degree to which systems are protected and the robustness of security mechanisms.

Pharming
Cyberattack aiming to redirect a website's traffic to another (bogus) website.

Phishing
Phishing attacks aim to gather confidential information by luring the user with a message which seems to come from a legitimate organization. Phishing attacks rely on social engineering and technical practices. The main motivation is financial gain. Phishers will either commit fraudulent acts with the collected information or they will sell it online in a public forum.

Phreaking
The illegal use or misuse of telecommunication services (by a phreaker) at the individual or operators' expense. The classic early example of phreaking was the use of cereal-box toy whistles which, when blown into a telephone handset, hit a pitch normally used to phone technicians to signal the system to allow free calls.

Piracy
An unauthorized duplication of goods protected by intellectual property law.

Port scanning
Sending a series of messages and queries to each port of the computer in order to obtain information on network services the computer provides, on the level of security and on which port numbers are opened. By scanning a computers' ports, the attacker will also be able to find weaknesses that will help him to break into the computer.

Prevention
Set of measures taken to avert a danger, a risk, aimed at preventing threats from materializing, at reducing the frequency of incidents with a view to protection.

Privacy protection
Protective measures to ensure that information on Internet user activities is not disclosed to any unwanted parties and is not used for purposes other than those to which the owner has consented. This refers to the right of individuals to verify the information concerning them that can be collected either directly, or indirectly by observing their internet behaviour and the sites they visit.

Private key
Key used in asymmetric encryption mechanisms (public-key encryption) that belongs to an entity and that must be kept secret.

Privilege-management infrastructure (PMI)
Infrastructure supporting management of privileges, authorizations and clearances.

Protection
The act of protecting, the state of being protected. Is said of a security measure that helps detect, neutralize or reduce the effects of an attack.

Proxy
A proxy is an intermediate agent or server that acts on behalf of an endpoint without allowing a direct connection between the two endpoints.
A proxy firewall (also applications level firewall) uses proxies to perform access control on the contents of packets and messages, as well as on attributes of the packet headers.

Public key
Generally speaking, in asymmetrical cryptography, an entity's public key must be made available to those who wish to send it encrypted data so that it can decrypt the data using the corresponding private key.

Public-key cryptography
An asymmetric encryption system that uses two-key ciphers, or a key pair: one is a secret private key, the other a public, publishable key. The two keys are complementary and indissociable. It is not possible to use the mathematical relationship between them to calculate the private key.

Public-key infrastructure (PKI)
Infrastructure supporting the implementation of asymmetric (public key) encryption, including, *inter alia*, management and distribution of encryption keys and digital certificates.

- Q -

Quantum cryptography
Quantum cryptography uses quantum mechanics to secure communications. At present, quantum cryptography is only limited to secret key distribution.

- R –

Reliability
A system's capacity to function without incident for a given period of time.

Repudiation
The fact of denying that one has taken part in all or part of an exchange.

Revocation
Notification that a private key has lost its integrity. The corresponding public key certificate must no longer be used. In respect of contracts, also refers to the right to withdraw an offer or acceptance of an offer.

Risk
The relative likelihood that a threat will materialize, measured in terms of probability and impact.

Risk analysis, risk assessment
Process of identifying and assessing risks (estimation of probability of occurrence and impact).

Risk management
Ongoing process of risk assessment conducted by an organization in order to control risks and keep them to an acceptable level. Can be used to determine the security policy best adapted to protect the organizations' assets.

Root kits
A rootkit consists of a set of software tools that help the attacker to mask intrusion, to hide running processes or system data and to gain access to the root whilst escaping detection.

Return on Security Investment (ROSI)
The point of maximum return on security investment is where the total cost of security is the lowest – including both the cost of security events and the cost of the security controls designed to prevent them.

- S -

Sabotage
A malicious act, vandalism, deliberate harm aimed at preventing an organization, an infrastructure, a service or a resource from operating normally; can result in losses.

Safety
The quality of that which is not harmful.

Sarbanes-Oxley
US legislation to ensure internal controls or rules to govern the creation and documentation of corporate information in financial statements. It establishes new standards for corporate accountability and sets penalties for corporate wrongdoings. Sarbanes-Oxley passed in 2001 in the wake of corporate accounting/governance scandals from big public companies including Enron, Worldcom and Global Crossing.

Secure Sockets Layer (SSL)
Software used to secure exchanges on the Internet, developed by Netscape and supported by most web browsers on the market.

Security
The situation in which someone or something is not exposed to any danger. Mechanism aimed at preventing a harmful event or at limiting its repercussions. **Physical security**,
for example, refers to the measures taken to protect environments physically or materially, whereas **logic security** refers to software procedures and means of protection.

Security administrator
Individual responsible for establishing or implementing all or part of a security policy.

Security audit
A methodical analysis of all security components, players, policies, measures, solutions, procedures and means used by an organization to secure its environment, conducted with a view to monitoring compliance, evaluating the fit between the organizational, technical, human and financial resources deployed and the risks incurred, and optimizing, rationalizing and enhancing performance.

Security measures
All technological, organizational, legal, financial, human, procedural, resources and means of action used to meet the security objectives established by the security policy. They are usually categorized by their functional role (preventive measures, protective measures, deterrent measures, etc.).

Security need
For an environment requiring protection, the identification and expression of levels of availability, integrity and confidentiality associated with the resources and values requiring protection.

Security policy
Security frame of reference established by an organization, reflecting its security strategy and laying down the means of implementation.

Security violation
An event, which may result in disclosure of sensitive information to unauthorized individuals, or that may result in unauthorized modification or destruction of system data, loss of computer system processing capabilities, loss or theft of any computer system resources.

Sensitivity
Characteristic of an entity indicating its value or importance.

Session key
Secret key generated using an asymmetric encryption system when the correspondents open a working session, and whose life span is limited to the session; the key is used to encrypt large volumes of data using a symmetric encryption algorithm.

S-http
Secure version of the http protocol that allows secure exchanges between a customer and a web server.

Sniffer
Software used to eavesdrop on data being transported on a network.

Sniffing
The act of passive eavesdropping in order to harvest connection parameters that are then used without the knowledge of their legitimate owners to commit unauthorized breaches.

Social engineering
Techniques, procedures and measures used by malicious attackers, who usually take advantage of the users' credulity to, *inter alia*, obtain their passwords and connection parameters and usurp their digital identity, in order to trick and breach the system by pretending to be authorized visitors.

Spam
An unsolicited electronic message sent in bulk, usually by email.

Spammer
Someone who engages in spamming.

Spamming
Technique involving the sending of unsolicited messages to an electronic message system.

Spear phishing
Spear phishing are more targeted attacks than lure phishing techniques. In order to launch these targeted phishing attempts, attackers have to collect or steal inside information to strengthen the feeling of legitimacy. For example, the phishing attackers will target a certain company, organization or agency and send a message that looks like it would come from a colleague or the employer.

Spim
Spim is a type of spam targeting users of Instant messaging services.

Spit
Spam over Internet telephony.

Spoofer
Someone who engages in spoofing.

Spoofing
Technique used to usurp IP addresses in order to breach a system.

Spyware
Program that sends sensitive information from the infected computer to the attacker. Spyware are programs that watch users' activities, gather information and transmit this information back to the creator of the spyware or the publisher without the users' knowledge. Spyware can represent a threat to privacy with more and more cases of identity theft, data corruption and personal profiling. Generally, spyware is bundled with another desirable program or downloaded in a peer-to-peer network.

Stalking
Repeated harassing or threatening behaviour in which an offender persistently contacts, follows, approaches, threatens or otherwise subjects a victim to unwelcome attentions.

Steganography
Technique used to hide an item of information within another in order to transport or store it covertly.

Surveillance
Continuous monitoring.

System intrusion
The entry of an external and unauthorized person or software into a system.

- T -

Threat
The possibility of trouble, danger or disaster.
Sign, indication, harbinger of a danger. Action or event liable to take place, to turn into an attack on an environment or resource and breach security. A person or thing that is likely to cause trouble.

Traffic analysis
Observation and study of information flows between source and destination entities (presence, absence, amount, direction, frequency, etc).

Transparency
The capability to watch and understand the functioning mode of a system, a software, or hardware.

Trapdoor see *Backdoor*.

Trojan horse
A malicious program hidden within a legitimate program and introduced into systems for the purpose of hijacking them (theft of processor time, corruption, modification, destruction of data and programs, malfunctions, eavesdropping, etc.). A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect. A propagating (or replicating) Trojan horse is a Trojan horse that creates a copy of itself.

Trust
The belief that somebody / something is good, sincere, honest.
Assured reliance on someone or something (a qualitative, subjective, highly relative criterion).

- U -

User charter
Document drawn up by an organization listing the rights, duties and responsibilities of its employees in respect of the use of the information technology and telecommunication resources it makes available to them, signed by the parties concerned.

User profile
List of user attributes that help to manage the network and systems to which the users are connected (identification and authentication parameters, rights of access, authorizations and other useful information) for the purposes of access control, billing, etc.

- V -

Virtual private network (VPN)
This concept refers to the use of IPSec to open a secure private communication channel over a non-secure public network. It is often used by an organization to connect its various sites via the Internet while guaranteeing the confidentiality of the data exchanged.

Virus
Malicious program introduced into a system without the users' knowledge. The program has the capacity to duplicate itself (either in identical form or, in the case of a polymorphic virus, by mutating), to damage the environment in which it is executed and to contaminate other users with which it is in contact. There are different kinds of viruses, depending on their signature, their behaviour, how they reproduce, how they infect machines, the malfunctions they cause, etc. **Worms, Trojan horses** and **logic bombs** are malicious codes belonging to the generic family of viruses.

Vulnerability
A security defect that could result in an intentional or accidental breach of security policy.

Victimology
A thorough study of all available victims information (age, sex, height, family, friends, acquaintances, education, personal habits, etc.).

- W -

Watermarking
Watermarking is a steganographic application that consists in placing indelible marks on an image.

Web and email spoofing
see Spoofing

Website defacement
Attack that consists of substituting original pages of a website with different pages or of disfiguring an original homepage by electronic graffiti pages. This attack is often used by hacktivists to spread political messages.

- Z -

Zombie
A system that has been hijacked by a criminal and utilized (without its owners' knowledge) to send spam or malicious codes and attack systems.

II. *Annex B – Some Web references (list not exhaustive)*

Some related Internet and computer security websites

www.enisa.europa.eu - ENISA -the European Network and Information Security Agency
www.cse.dnd.ca - Communications Security Establishment. Canada's National Cryptologic Agency
www.dsd.gov.au - Defense Signals Directorate – Australian Government – Departement of Defence
www.nsa.gov - National Security Agency (USA)
www.eema.org/ - The European Forum for Electronic Business (EEMA) – The independent European association for e-business
www.first.org - FIRST (Forum of Incident Response and Security Team)
www.cesg.gov.uk - National Technical Authority for Information Assurance (UK)
www.europa.eu.int/information_society/index_en.htm - Europe's Information Society Thematic Portal
www.melani.admin.ch - Computer and Internet security (CH)
www.cert.org - CERT – Center of internet security expertize, Carnegie Mellon University (USA).
www.apcert.org - Asia Pacific Computer Emergency Response Team
www.jpcert.or.jp/english/index.html - Computer Security Incident Response Team Japan – Supporting the Internet security in Asia
www.auscert.org.au - AusCERT – Australia Computer Emergency Response Team
www.niser.org.my - National ICT Security & Emergency Response Centre – Malaysian Computer Emergency Response Team
https://www.cert.ru - CERT – (Russia)
www.wikayanet.dz - Algerian Portal of Information Security
www.crime-research.iatp.org.ua - The Computer Crime Research Center (CCRC) Ukrainian branch
www.crime-research.ru - The Computer Crime Research Center (CCRC) Russia
www.clusif.fr - Club de la Sécurité de l'Information Français
www.cs.purdue.edu/coast/coast.html - COAST (Computer Operations, Audit and Security Technology)
www.hoaxbusters.ciac.org - Information about hoaxes
www.spamfighter.com/Default.asp - Information about spam
www.ripe.net/ripe/wg/anti-spam/index.html - Anti spam working group
www.secuser.com - About anti-spam anti-intrusion, privacy
www.antiphishing.org - Anti phishing working group
www.oecd.org/dataoecd/29/12/35670414.pdf - OECD Task Force on Spam report Anti Spam Regulation released in November 2005
www.oecd-antispam.org - OECD toolkit on spam
www.aptsec.org/meetings/2005/NSS/docs/index.htm - Symposium on Network Security and SPAM (22 - 24 Aug. 2005, Jakarta, Indonesia)
http://wiki.apcauce.org/index.php/Main_Page - APCAUCE, the Asia Pacific Coalition Against Unsolicited Commercial Email

Some related Internet law issues websites

www.cybercrimelaw.net - Cybercrimelaw.net is a global information clearinghouse on cybercrime law (Norway)
http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm - Convention on Cybercrime – Budapest, 23.XI. 2001 – Council of Europe
www.legi-internet.ro/en/cybercrime.htm - Romanian IT Law
www.wipo.int/portal/index.html.en - World Intellectual Proprety Organization
www.ilrg.com - Internet Legal Research Group
www.cyberlawinformer.com - Legal Issues on Internet
www.cybercrimelaw.net - Cybercrime Law web site give a comprehensive survey of current legislations from around the world includes the laws of 78 countries.
www.legalis.net - Jurisprudence, current events and Internet law

www.foruminternet.org - Information dedicated space about the legal issues concerning Internet end network
www.cybercrimes.net - The University of Dayton – School of Law (USA)
www.gseis.ucla.edu/iclp/safe.htm - The UCLA Online Institute for Cyberspace Law and Policy (USA)

Some related privacy protection issues websites
www.privacyinternational.org - Privacy protection
www.privacy.org - Privacy protection
www.w3.org/P3P/ - Platform for Privacy Preferences (P3P) Project
www.cyberrights.org - Cyberrights &cyberliberties protection
www.epic.org - Electronic privacy Information Center

Some computer crime related issues websites
www.ic3.gov - Internet Crime Complaint Center (IC3) (USA)
www.nw3c.org - National White Collar Crime Center (NW3C) (USA)
www.cyberwise.ca/epic/internet/incyb-cyb.nsf/en/Home - National Strategy for the Protection of Children from Sexual Exploitation on the Internet
www.cybercrime.gov/cc.html - Computer Crime & Intellectual Property Section/United States Department of Justice
www.crime-research.org - The Computer Crime Research Center (CCRC)
www.fraud.org - National Internet Fraud Information Center
www.idtheftcenter.org/index.shtml - Identity Theft Resource Center (ITRC)
www.oecd.org/fatf/ - Financial Action Task Force (FATF-GAFI)
www.uncjin.org - United Nations Crime and Justice Information Network

Some law enforcement related issues websites
www.rcmp-grc.gc.ca/scams/ccprev_e.htm - The Royal Canadian Mounted Police
www.interpol.int/ - Interpol – international police organization
www.interpol.int/Public/FinancialCrime/default.asp - Interpol – Financial and High-tech crimes
www.htcia.org/ - Internet High Technology Crime Investigation Association
www.cybercellmumbai.com - The Cyber Crime Investigation Cell of Mumbai Police India
www.scoci.ch - The Swiss Coordination Unit for Cybercrime Control

Others websites of interest
www.wikipedia.org - Wikipedia: the free encyclopedia
www.intgovforume.org - Site of the Internet Governance Forum (IGF)
www.oecd.org - OCDE website Organization for Economic Co-operation and Development - Information Security and Privacy
www.saferinternet.org - Europe's Internet Safety portal
www.warp.gov.uk - Warning, advice and reporting point (UK)
www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/ - Actions against Economic and Organized Crime – Council of Europe