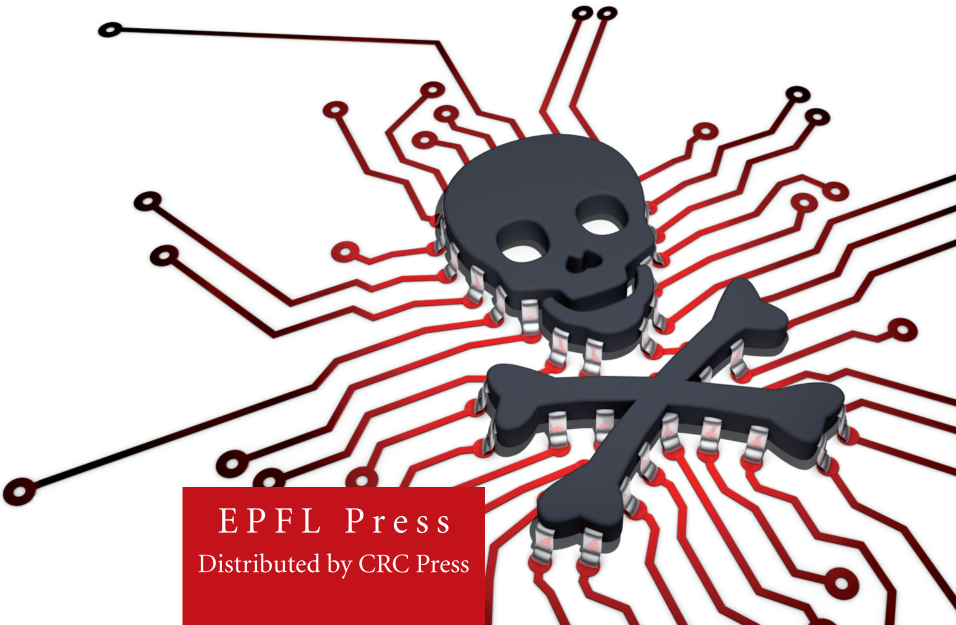
CYBER POWER

CRIME, CONFLICT AND SECURITY IN CYBERSPACE

Solange Ghernaouti



EPFL Press
Distributed by CRC Press

CYBERPOWER

Cover Illustration: © asrawolf - Fotolia.com

Forensic Sciences

CYBER POWER

CRIME, CONFLICT AND SECURITY IN CYBERSPACE

Solange Ghernaouti

EPFL Press
A Swiss academic publisher distributed by CRC Press

EPFL Press
Presses polytechniques et universitaires romandes, EPFL
Post office box 119, CH-1015 Lausanne,
Switzerland
E-Mail:ppur@epfl.ch, Phone: 021/693 21 30, Fax:
021/693 40 27

Taylor and Francis Group, LLC
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487
Distribution and Customer Service
orders@crcpress.com

EPFL Press ia an imprint owned by Presses polytechniques et universitaires romandes, a Swill academic publishing company whose main purpose is to publish the teaching and research works of the Ecole polytechnique fédérale de Lausanne.
Version Date: 20130927

International Standard Book Number-13: 978-1-4665-7305-5 (eBook - PDF)

The authors and publishers express their thanks to the Ecole polytechnique fédérale de Lausanne (EPFL) for its generous support towards the publication of this book.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Table of Contents

Preface and Acknowledgement

Cyberspace has become the environment in which new forms of crime are committed, as well as the economic and military battlefield where conflicts of all kinds are being played out. The control of information and telecommunication infrastructure, with the ability to respond to cyberattacks and to ensure cybersecurity, offers real power and is already one of the most significant political, economic and technological issues of the twenty-first century. Cyberpower has become the newest means for organisations, both legitimate and criminal, to demonstrate their capabilities. Information and communication technologies (ICT) have grown to become a critical part of our society's infrastructure, and their potential misuse affects us all, from the individual citizen to private and public organizations and to states.

This book explains how the concept of cyberpower rises naturally from a holistic consideration of cybersecurity and, specifically, how it can be expressed through cybercriminality, cyberterrorism, cyberconflicts and cyberwarfare. It evaluates the impacts on – and the consequences for – individuals, organisations and states. It provides a panorama of the actors and their means of operating, with a description of the strategies, methodologies and kinds of measures that can be employed to combat the abusive and criminal use of digital technology and to improve security in both cyberspace and real life.

The book Cyberpower describes how to master cyberrisk at the national and international levels, starting with an overview of the general issues before presenting the main themes from the perspectives of all the actors involved (Figure 1).

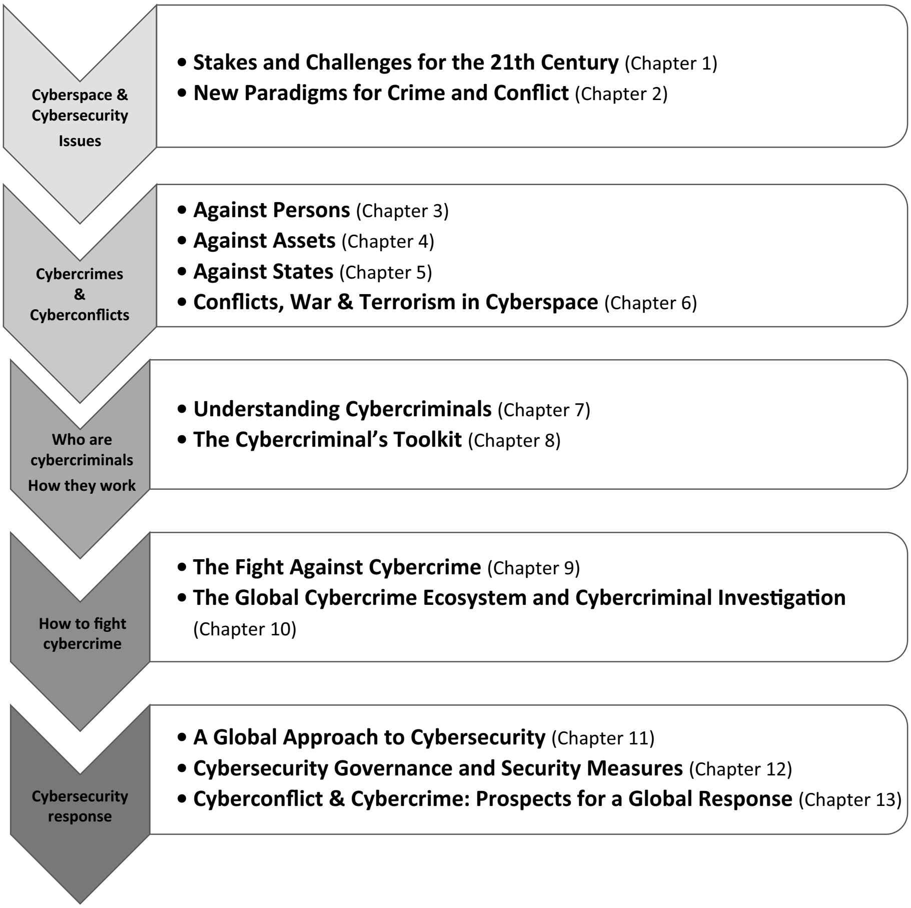

Cyberspace & Cybersecurity Issues
• Stakes and Challenges for the 21th Century (Chapter 1)
• New Paradigms for Crime and Conflict (Chapter 2)
Cybercrimes & Cyberconflicts
• Against Persons (Chapter 3)
• Against Assets (Chapter 4)
• Against States (Chapter 5)
• Conflicts, War & Terrorism in Cyberspace (Chapter 6)
Who are cybercriminals How they work
• Understanding Cybercriminals (Chapter 7)
• The Cybercriminal's Toolkit (Chapter 8)
How to fight cybercrime
• The Fight Against Cybercrime (Chapter 9)
• The Global Cybercrime Ecosystem and Cybercriminal Investigation (Chapter 10)
Cybersecurity response
• A Global Approach to Cybersecurity (Chapter 11)
• Cybersecurity Governance and Security Measures (Chapter 12)
• Cyberconflict & Cybercrime: Prospects for a Global Response (Chapter 13)

Figure 1 The structure of the book as a flow diagram.

The chapters have been written to follow a consistent structure based around topics such as: understanding the context; the facts; the background; the challenges; and practical examples (taken from the field or rendered anonymous); Chapters also include a summary, exercises, and occasionally, case studies.

Our perspective and approach to crucial cyber-related issues are non-political, non-partisan and non-governmental. The emphasis is placed on pedagogical quality to propose high-level syntheses – often graphically – and to provide a consistent treatment of various cyberrisk-related domains from the full range of perspectives of those most implicated (civil and military; private and business). Highly technical issues are explained so that all interested people, even those with minimal computer training, can understand how cyberattacks are carried out and why they are effective. Fundamental principles are explained through an interdisciplinary and transversal approach that reflects the societal, economic, political, legal, military and technical issues related to the uses and misuses of information and communication technologies.

The objective of this work is not to incite the reader to commit cybercrimes. Its role is to contribute to the understanding of the threats that society should be prepared to face and of the ways in which crimes and conflicts are carried out in cyberspace. Its main objective is to participate in developing the awareness and skills that will allow society to fight against cyber-based criminality and abuse. The examples given in this work are designed to illustrate concepts, not to praise specific actions or to single out any specific person, organisation or state. Examples based on genuine cases of cybercrime are not exhaustive and are not intended to emphasise any given weakness or denounce those who have been victims of cybercrime. These examples do not constitute any incitation to commit such a crime. Indeed, our examples have been selected in full knowledge that many other organizations and countries have been subject to cybercrime, and that many other similar stories could be told.

Solange Ghernaouti, October 2012

Acknowledgement

The author wishes to signal her gratitude and to offer her thanks and appreciation to her colleague David Simms of the University of Lausanne, a native English speaker for his patience and assistance in reading draft versions of this work making comments and offering advice on emphasis and phrasing.

Dedication

I would like to dedicate this book to the people making their best efforts to fight against cybercrime and the misuse of ICT all around the world.

A special thanks is addressed to Judge Stein Schjolberg, Chairman of the High Level Expert Group of the ITU Global Cybersecurity Agenda, with whom I had the opportunity to work closely as work area leader for the Global Cybersecurity Agenda. Since that time we have continued to work together to promote peace and stability in cyberspace and in real life.

Foreword

If you were to see, in the street in front of you, a battle tank carrying the flag of an enemy country, you would recognize it immediately and know its intentions. If, on the other hand, you encountered a piece of malware, it is highly likely that you would not notice anything at all. And even if by chance you did detect – and even better – identify the piece of malware, you would almost certainly be unable to say who was the author, who was using it, or what their intentions were. Might it be the beginning of an attack or the final phase of one? Could it be an act of war? Perhaps it is the child next door taking tentative early steps as a script kiddie? Or maybe a bridgehead created by a criminal organisation looking to empty bank accounts? Could it be related to the theft of industrial secrets?

In contrast to classical conflicts, attacks in cyberspace (and malware is just one type among many others) are very difficult to classify. It is necessary to employ a multi-criteria approach to be able to distinguish between, on the one hand, a criminal act infringing a penal code and on the other an attack launched by one state against the sovereignty of another and impacting the laws regulating the relationships between them. Among other things, it will be necessary to determine to whom the attack can be attributed, which methods are used, what the objectives are, and what the nature and extent of the damage caused has been.

There is a massive challenge in finding appropriate answers to the multiple and diverse aggressive acts that are perpetrated daily in cyberspace. Three trends make this even more complicated:

- Technological evolution: our infrastructure, the objects we use every day, and even living beings are becoming ever more interconnected and interdependent, and as technology is never exempt from flaws and users are equally imperfect, the omnipresence of information technologies will bring with it an explosion of vulnerabilities and therefore of additional risks.
- Human evolution: we are becoming "Homo cyberneticus," dependent beings whose behaviours are being modified at a very deep level; at the rate at which things are developing, private spaces may find themselves without protection.
- The evolution of violence: trends in both the technical and human spheres will create opportunities for all kinds of attacks. Cross-border criminality, ever more present, efficient and professional, will benefit increasingly from the weaknesses that have been created. In the same way, cyberspace will be intensively and more frequently used in the context of political struggles; indeed, we can count on cyberterrorism becoming a reality. And after having understood at the beginning of the twentieth century how to use airspace, armies will now consider cyberspace as a specific domain for war, thereby changing it profoundly.

As these few lines have illustrated, analysis of cyberrisk in the context of one homogenous category would be a grave mistake. In order to understand and combat cyberattacks, it is necessary to assess this field from a global perspective: this is the approach that has been chosen by Solange Ghernaouti. First of all, she systematically depicts cyber-equipped aggressors, along with their methods and the stakes at play; and she then describes the solutions that can be employed, clearly reminding the reader each time of the context in which these attacks are taking place.

Information technology is omnipresent, but considering cyberspace purely through the optic of technical considerations would be a major error. Here again Solange Ghernaouti avoids the trap of making readers believe that defence against cyberattacks is simply a matter for geeks. In reality, it requires a complex effort that draws upon multiple competences, and it is this that emerges most strongly from this book; a book that will surely become a standard reference work for many, in particular for managers who must understand the stakes related to cyberrisk in order to make good decisions.

Considering the certain growth of cyberrisk we are faced to some extent with an uncertain future. But with this book, Solange Ghernaouti has provided an extremely important tool that will allow us to continue to benefit from all the advantages that cyberspace has to offer. We should heed her advice.

Gérald Vernez (col. GS)
Delegate of the Chief of the Swiss Armed Forces for Cyber Defense
(Former Deputy Director of the Swiss National Cyber Defense Project)

Chapter 1

Cybercrime and Cybersecurity Issues: Stakes and Challenges for the 21st Century

1.1 Understanding the context

The facts

Citizens into have been robbed, children in danger, ruined corporations, threatened states – cybercriminals are spreading their influence as fast as the Internet is developing. Since we do not see or know them, we inadvertantly trust cybercriminals, thus giving them their strength. No one is immune. Whether via the manipulation of opinion, spying, identity theft, terrorism, harassment, swindles, financial fraud or various types of crimes, cybercrime touches all of society. By simply using services offered by the Internet, users are vulnerable to criminal threat and can become a victim or an unwilling author of a crime. Cybercrime has become a reality of contemporary life. It has had greater or lesser consequences for people, organizations and states, but over a few short years, it has grown into a veritable plague on society.

Information and communication technologies (ICT) allow huge amounts of information to be stored, processed, accessed, searched, transmitted, exchanged, and disseminated, regardless of geographic distance. These unprecedented possibilities lead to new services that can improve economic development and the dissemination of knowledge. But at the same time, new types of crime have appeared, as well as old crimes committed with new technologies (Figure 1.1). Spam, computer viruses, cyberattacks, and identity theft, for example, increase in frequency by the day.

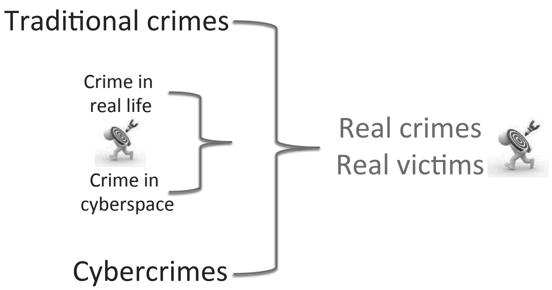


Figure 1.1 Cybercrime is an extension of ordinary crime.

Internet technologies are facilitators for many kinds of infringements: theft; sabotage of information; copyright infringements; breach of professional secrecy, digital privacy, or intellectual property; dissemination of illegal contents; competing attacks; industrial espionage; breach of trademark laws; dissemination of false information; denial of service; various frauds; money laundering – the list of possible offences goes on. Information technology resources have become the potential hostages of cybercriminals. Thus, organizations can no longer neglect these real dangers and must accept the need to protect their infrastructures, their processes, flows, and information. They must be prepared for the threat of cybercriminality, a threat that one day may become reality.

Some examples from the press

Cybercriminality is a reality of the world today. Not a day goes by without mention in the media of incidents relating to cybercriminal activities, as the examples below indicate.

From the media

Case 1

After Anonymous ransacked think tank Stratfor's computers and stole away thousands of credit card numbers and other personal information, it claimed to have also clipped the company's confidential client list. That list contains sensitive information about Stratfor's high- profile clients, such as Apple, the U.S. Air Force, and the Miami Police Department. However, Stratfor denies that Anonymous got the think tank's family jewels. […][1]

[1] Source: Computerworld – John P. Mello Jr., 26 December 2011. http://www.computerworld.com/s/article/9223025/Confidential_client_list_safe_from_Anonymous_Stratfor_says?taxonomyId=82

Case 2
Four residents of Romania have been charged for their alleged participation in a multimillion-dollar scheme to remotely access point-of-sale systems at more than 150 Subway restaurants and other U.S. merchants and steal payment card data, the U.S. Department of Justice said. […] The four-count indictment, unsealed Wednesday, charges the four Romanians with conspiracy to commit computer fraud, wire fraud and access device fraud. Charged in U.S. District Court for the District of New Hampshire […][2].

Case 3
The U.S. can expect more aggressive efforts from countries such as Russia and China to collect information through cyberespionage in areas such as pharmaceuticals, defense and manufacturing, according to a new government report released Thursday[3]. […] D.C. was an engineer with Rockwell and Boeing and was sentenced in 2010. He worked on the B-1 bomber program and was found to have 250,000 pages of documents in his house, which would have filled four, four-drawer filing cabinets. If converted to digital format, the information would fit onto one CD. “Cyberspace makes possible the near instantaneous transfer of enormous quantities of economic and other information,” the report said.[4]

Case 4
Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts. The cost to Sony and credit card issuers could hit $2 billion […] Sony Computer Entertainment and Sony Network Entertainment acknowledged that an ‘unauthorized person’ has stolen the following kinds of information that was provided by its by PlayStation and Qriocity customers: “Name, address, country, email, address, birth date, PlayStation Network/Qriocity password and login and handle/PSN online ID.”[5]

[2] Source: Computerworld IDG News service – Grant Gross. 8 December 2011. http://www.computerworld.com/s/article/9222520/Four_charged_with_hacking_point_of_sale_computers?taxonomyId=82

[3] Report to Congress on Foreign economic collection and industrial espionage, 2009 – 2011. Office of the National Counterintelligence Executive (USA) – October 2011.

[4] Source: NetworkWold – IDG News Service. Jeremy Kirk. 3 November 2011. http://www.networkworld.com/news/2011/110311-us-report-warns-of-russia-252717.html?hpg1=bn

[5] Source: NetworkWold – Jeff Vance. 3 October 2011. http://www.computerworld.com/s/article/9220459/The_future_of_malware?taxonomyId=82

The background

The standardization of the computing and telecommunication worlds by the global adoption of Internet technologies, the dependency of organizations and states on those same technologies, as well as the interdependency of critical infrastructures, make society vulnerable to computing crimes and cybercrime. The insecurity generated by computing – criminal or not – can no longer be ignored. There is a need to rethink the security of individuals, organizations and states with reference to the possible risks. In general, three different approaches can be adopted: accept, transfer, or control the risks. In an information society, acceptance would constitute a huge mistake; however, the idea of being able to transfer computing risks is downright utopic. That leaves one option. We have to control the risks by developing an educated culture regarding security, while respecting the democratic values of our society.

Cybercrime forms a continuation of classic criminality wherein the computer, with the programs and data that are inside and the networks it uses, can become both a target of an attack and a means of carrying one out (Figure 1.2).

Cybercrime benefits its sponsors. Organized crime has quickly understood how to take advantage of information and communication technolo-

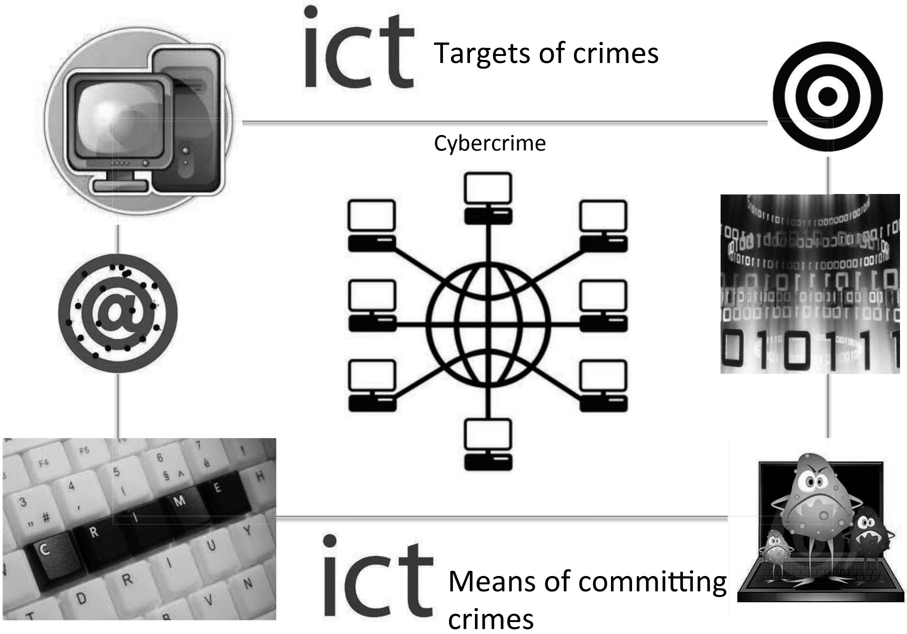


Figure 1.2 Electronic devices, telecommunication networks, and data as the means and targets of crimes.

gies to communicate, organize, and identify both victims and opportunities, thereby increasing efficiency in drug and human trafficking, illegal commerce of rare or protected species, money laundering, selling of counterfeit products, or other economic crimes. As a side effect, criminality also benefits legal enterprises that take advantage of insecurity, such as antivirus or anti-spam providers, vendors and consultants of computing security products, without forgetting those who:

- generate fear in order to destabilize, manipulate, sell, or influence decision processes with different objectives;
- sponsor attacks to increase security budgets where they find a certain benefit;
- directly benefit from the overflow of information generated by spamming (Internet, storage and infrastructure providers);
- enrich themselves from money laundering;
- take advantage of industrial spying performed through the Internet or of actions against a country or institution's image.

The synergy and the convergence between mob crime, economic crime, and cybercrime require a complete multilateral and transnational answer to satisfy requirements for protecting national security, organizations, or individuals. This answer will be linked to the sensitization of the actors to the stakes of controlling security, to the criminality in question, and to the elementary precautions that, if clearly announced and defined and intelligently used, will reinforce the actors' confidence in ICT technologies while limiting criminal opportunities.

Cybercrime is not only a matter for international awareness, the subject of political and judicial debates, and the basis for technological, sociological and economical research, but also an issue that concerns everyone and cannot be understood from one single perspective, or apprehended in a unique dimension, be it legal or technical. Only an interdisciplinary approach to the phenomenon of cybercriminality leads to the understanding required to define appropriate preventive and reactive measures.

The challenges

Fighting effectively against cybercrime requires a strong political position that brings together public and private bodies and mobilises them to work together nationally and internationally. Let us hope that such collaboration could be operational quickly, given the stakes of the war against cybercrime, and the way that success would benefit the whole of society and the economic stability of a country.

"We do not inherit the Earth from our ancestors, we borrow it from our children," remarked Antoine de Saint-Exupéry. In a similar way we have not inherited the Internet or cyberspace in general, but are building it for our children. We have to be participants, aware that the information society is under construction, aware that changes are being driven by the commercial logic of information technologies. This understanding will oblige us to ask ourselves what we can expect and accept from these technologies and of the criminality that they permit (Figure 1.3).

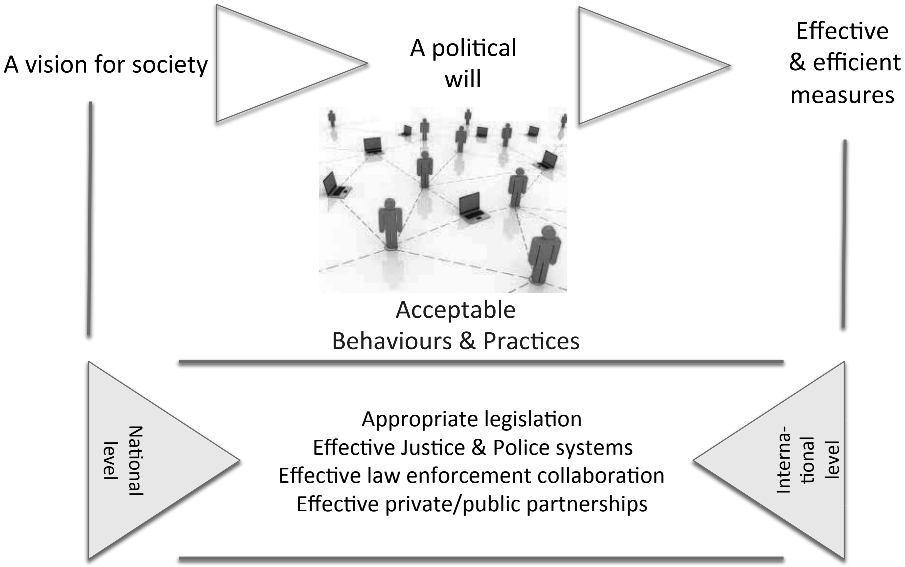

A vision for society
A political will
Effective & efficient measures
Acceptable Behaviours & Practices
National level
Appropriate legislation
Effective Justice & Police systems
Effective law enforcement collaboration
Effective private/public partnerships
Interna-tional level

Figure 1.3 Main challenges to be answered when fighting against cybercrime.

Information security is a matter of state sovereignty, national security, the cultural heritage of nations, and the protection of critical infrastructure, systems, networks, goods and values. As of recent years, the computer has also impacted personal security.

While technical security measures have to be developed and implemented, concomitant legal measures have to exist to prevent and deter criminal behaviour. In the general context of dependencies and interdependencies of ICT infrastructures, society has to have an effective justice and police system in order to master computer related crimes.

It has become imperative that states not only introduce measures to fight against cybercrime, but also to control the security of their information technologies infrastructures. Information security and cybersecurity constitute a driving force for the economic development of regions and must be implemented simultaneously with the development of the infrastructure. Organizing the protection and defence of the values of our information society must account for criminal threats and the growing convergence of organized crime, economic crime, and cybercrime. A comprehensive, multilateral, international response is required, and it must satisfy the security needs of countries, organizations and individuals.

Many different points of view, needs, and participants should be taken into consideration in order to find an acceptable compromise between “freedom” and “security.” It is also necessary to take up the challenge of simple and effective security as opposed to the complex environment in which security must be implemented. It is not necessary to search for “best practices,” but rather find good practices for each participant, including law enforcement activities.

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 multi-dimensional and multi-stakeholder approach for everyone – from individuals to organizations to states.

Cybercrime is not restricted by geographic or national boundaries. A criminal can be located in a country different from the one in which the crime is committed. This presents a fundamental legal question in light of technical possibilities. Domestic laws are confined to specific territories, but electronic exchanges or data flows do not know any geographic boundaries. The only possible answer is to address legal issues related to cybersecurity and cybercrime at an international level. Within the context of the Internet and cyberspace, it is essential to adopt adequate international frameworks and instruments that respect human rights.

Too often, the complexity of technology benefits cybercriminals. However, this is not an insurmountable problem. Even if the security solutions available are sometimes fallible, this book demonstrates that it is wrong to think that we are unarmed against this new criminality. Largely illustrated by real cases, it proposes a clear synthesis of what cybercriminality is and the means by which it is carried out. It presents key methods for learning how to identify threats, to avoid risky behaviour and to discover multiple forms of cybercrime on the Internet. This book also provides pragmatic answers for people who use the Internet for private or personal reasons and have concerns about risks, threats and security.

1.2 The risks and the needs

The global dimension of risks related to cybercrime

Criminal risks carry a global dimension that can impact every aspect of an organization – all of its stakeholders. The organization has to know how to preserve its integrity against the criminal, just as it protects itself, for example, from corruption. It has to remain profitable and in its planning account for any loss of profits due to addressing the risk of cybercriminality – that is, the costs involved in providing counter-measures (Figure 1.4). There is a need to develop a financial model that will optimally support the costs of protecting the infrastructures and of securing the systems, networks, data, services and people, and indeed every asset and key attribute of a business or public agency. This kind of model not only will inevitably have an impact on the costs of production but also will contribute to continuing the development of business activities through the appropriate application of the organization's assets.

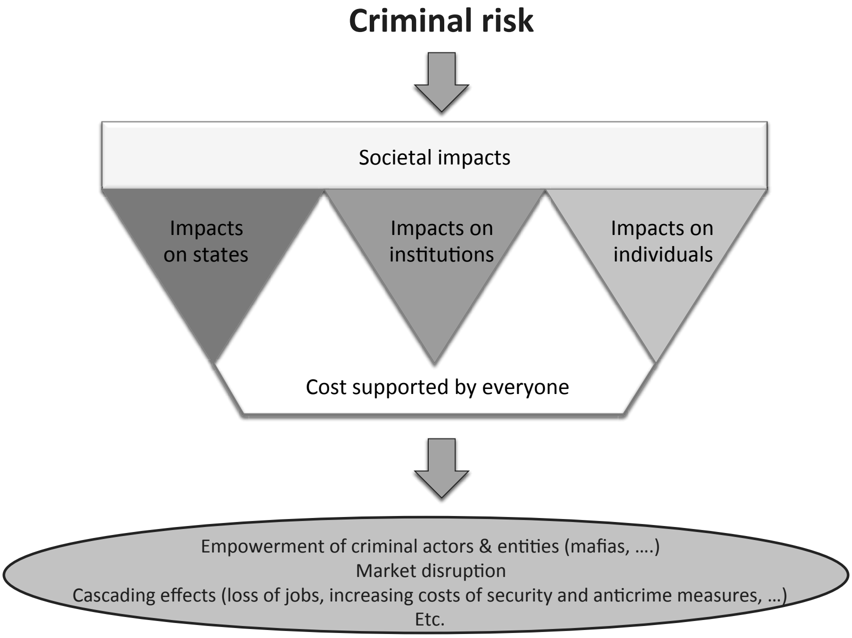

Criminal risk
Societal impacts
Impacts on states
Impacts on institutions
Impacts on individuals
Cost supported by everyone
Empowerment of criminal actors & entities (mafias, ….)
Market disruption
Cascading effects (loss of jobs, increasing costs of security and anticrime measures, …)
Etc.

Figure 1.4 The global dimension and cost of cybercrime

Organizations can no longer neglect the real dangers that threaten them. They are aware that they have a pressing duty to protect their ICT's infrastructures, data, information flows, industrial and commercial secrets, and their finances. They have to be prepared for the cybercriminal threats that might one day come to pass.

It is necessary to disseminate a culture and a multidisciplinary approach to both security and the handling of computer-related crimes. For entities such as states, their dependency on information processing technologies, associated with the interdependency of the necessary infrastructures and the inherent vulnerabilities of the computer systems, means that they require a global, strategic vision to address this problem. Organizations and, indeed, society at large must be equipped with measures, procedures, and tools that allow the efficient management of technological and information-related risks.

A market in complete expansion

There is no lack of resources in the field of security. The security market is in perpetual expansion. But are the services and products on offer really adapted to the consumer's needs? Are they properly implemented and managed? These questions persist as a result of their relevance to an environment undergoing perpetual mutation with a human dimension that is difficult to manage. Some of the worst consequences arise from simple human issues such as deficient management, casual negligence (the password written on a scrap of paper stuck to the screen), incompetence (mistakes when the technology is developed or implemented), or even too much power granted to system administrators.

Furthermore, commercial entities will tend towards avoiding the costs of security. Indeed, it can even be more profitable, for some economic actors that are not legally obliged to provide secure solutions, to pass such costs on either to the consumer (through the need to purchase supplementary products, undergo training, or replace infected or compromised materials) or to society in general. The latter case applies, for example, in the event of a business making its staff redundant after becoming insolvent due to a security failure or a computing attack.

While employing politically advantageous speech that encourages the participation of the private sector in the war against cybercrime (which in some cases has gone as far as offering colossal rewards to incite people to provide information leading to the arrest of a cybercriminal – a kind of *cyber Far-West*), these actors continue to sell computing solutions that include security failures; however, because they are computer solutions, they have no guaranteed robustness and often contain exploitable vulnerabilities.

Above the responsibility of the end-user

The current tendency is to place responsibility for security with users, without, however, providing them with the means to control the security of their data, which might be voluntarily passed to third parties or simply stolen. The possibility or even necessity of obtaining a kind of Internet driver's licence is sometimes evoked to try to ensure that users do not encourage the development of cybercrime. We need to remain aware, however, that a driving licence has never prevented antisocial or risky behaviours. Nevertheless, it is necessary to develop a computing mindset in order to know how to avoid being an easy victim for a cybercriminal, to understand what constitutes dangerous attitudes or behaviours, and to increase the quality of the security that protects users.

By analogy, it is not the information campaigns against AIDS alone that will stop the spread of the illness. It is not because a person uses condoms that he can avoid infection by a contaminated blood transfusion. Continuing with the AIDS analogy, a woman taking all reasonable protections, as indicated in the prevention campaigns, and who never puts herself in a risky situation nor will ever need a transfusion, will probably never be infected and will not contribute to the transmission of the plague – unless she is raped by a HIV-positive person.

There is no way for individual to completely master the whole chain of information processing and communications. It is not simply through being informed that he will not have an ICT security problem resulting from elements beyond his control. Let us imagine, for example, a well-informed Internet user (someone educated who has acquired specific training), who does not use social networks, who never transmits his personal data (he knows he must never answer a spam or different requests for information), who keeps his antivirus software up to date, who refuses *cookies* when the access to a website requires the installation of a small program[6]; who employs a specialist to keep his machine clean, who refuses targeted advertising, who never downloads or copies illegally any data (movies, music,…), who always purchases the software he is using, who never goes onto auction or pornographic websites, who never plays on virtual casinos, etc. This person can still be a victim of cybercrime. Indeed, his personal data will inevitably be distributed between different administrative and corporate websites (Internet service provider, insurance company, local administration, dentist, doctor, travel agency, bank, etc.), over which he has neither control nor assurance that they are well protected.

[6] A *cookie* is provided by a web server and can collect information and transmit it, against the user's will

Taken to extremes, the end logic of user responsibility would be to forbid him from using the Internet. The advice we should give him would be:

- firstly: never connect your computer to the Internet;
- secondly: do not communicate; and
- thirdly: never use e-services or websites, even official ones.

On the other hand, if he is appropriately educated, and if security measures are provided to him at a reasonable price, and if these tools are understandable and easy to use, the user will certainly not become a transmission agent, an active driver or target of cybercrime. But as always, the most deprived suffer from security failures, starting with individual users, youngsters, and then small and medium-sized enterprises. Security is not solely weakened by the consumer's inability to use a computer or network correctly, even if properly trained.

Cybersecurity affects everybody by way of the services, products, solutions, pieces of equipment, and other elements provided through the Internet. Each participant has to assume part of the shared responsibility. Each must stop transferring security responsibilities onto other entities and start discharging them himself.

We need not only technological and political security solutions, but also laws. A law that does not address the problem is not only useless, but also it carries a significant cost for society. In order to be efficient, laws need organizational, human, technical, and financial resources must be applied in order to: start investigations on computing crimes, prosecute cybercriminals and indemnify victims. These laws will also have to be the result of an international effort to combat cybercrime, since it is a transnational plague. Radioactive clouds do not stop at national borders and neither does cybercrime!

In this context educating consumers is a necessary but insufficient part of the solution, and expecting the user to bear the costs and responsibility for security would be unfair. Individual users cannot reasonably be expected to stop using the Internet, particularly when considering the number of services that have disappeared from the offline world and are now only available on the Internet. This has come about because such online services add value for the consumer (who does not have to move from his current location) and for the provider (in savings in property, costs, and salaries). Nowadays, a consumer really has to make an effort not to consume a service or acquire a product over the Internet: from photo development to banking and other counter services that are no longer offered, since everything can be done through the Internet.

If no online services were available, we would need to rethink the ease of customer service, by reopening counters and keeping them available at fixed and long hours, as with the Internet which provides services anytime and from everywhere. Overall, in terms of providing personalised, high quality service for the consumer, this would not necessarily be a bad thing. But even were this to come about, there would still be electronic transmissions from the physical customer service desk to networked systems, and these transmissions would need to be secured. In this context, security would remain the responsibility of the service provider rather than the consumer, and the consumer would always retain the option of changing service provider in the event of any problems.

A long-term vision

Why is it that instead of entering into a technological race to find counter-measures, a race that has already been lost because the criminals always have a head start, we do not simply take the time to think about the significance of our Internet dependency? Why are we not considering the "opportunity" dimension of cybercrime risks?

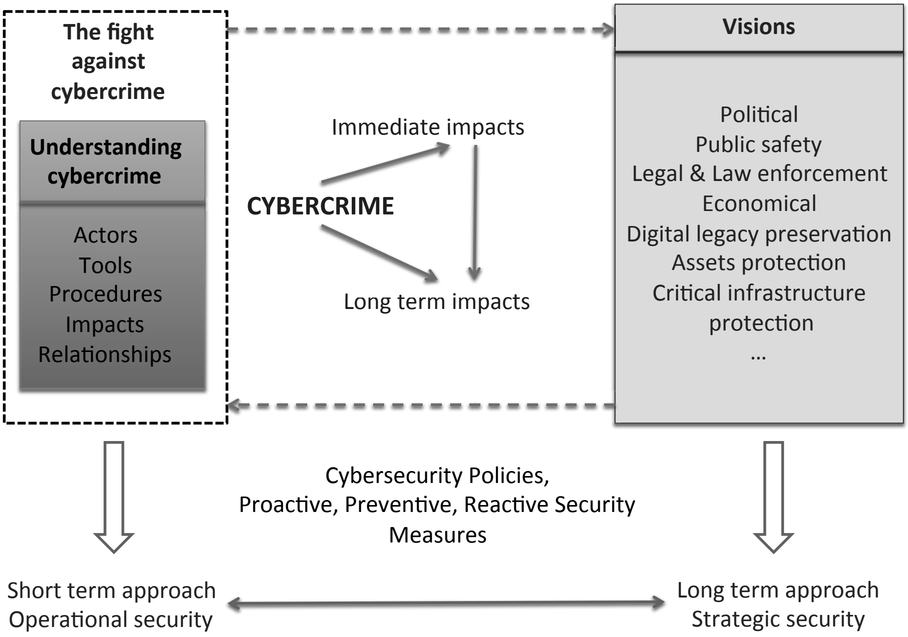


Figure 1.5 Needs for a long-term vision.

We need to combat cybercrime, but without losing our individual freedoms or our right to privacy. It would be advisable to prevent the emergency and unthinking adoption of legal or technological measures that could harm democratic values and the fundamental rights of citizens, and that could prove in the long-term to be ineffective for individuals' security and the protection of assets (Figure 1.5). We should not underestimate the will of some states and actors (the most powerful ones) to impose their own preferred ways of providing security through their technologies and laws, under the pretext that this problem needs to be solved quickly. There is a great temptation in urgent situations to adopt devices and technologies controlled by foreign countries, and this could lead to a country in some sense losing its competencies, its autonomy, its capacity to plot its own course in respect of culture and specific know-how, and finally its sovereignty, by becoming the hostage of judicial approaches to security and IT technologies imposed by others.

To the extent that the Internet has become, rightly or not, a major constituent of the global economy, does it not constitute an element of critical infrastructure much like the electricity distribution system? Indeed, the ability of businesses to create wealth and to develop services is increasingly linked to ICT technologies. In addition, ICT infrastructures belong to those who rely on them. Even the "public" infrastructures belong, primarily, to private entities. In this context of the dependency on and interdependency of computing and electrical infrastructures, who, in the end, is responsible for security? Is it more judicious to talk of cybersecurity or critical infrastructure security?

Is it only a matter of terminology, or is it a genuine movement in the stakes, scope, and market of the application of security? It is hard to answer this and to identify the challenges that leaders will need to address in relation to the management of the risks related to security and computing. It is temptating to change the focus of research without even answering the fundamental inherent question: who controls security?

The answer to this question will necessarily include the answers to other serious questions as for example:

- How can security be guaranteed?
- What degree of confidence can we have over tools and services created by other people?
- To what extent can ITC risk be covered by insurance?
- What are the tools, methodology and competencies necessary for understanding computing risk in order to apply efficient and coherent security measures that will allow the management of this risk or its transformation into business opportunities?

These are open questions that climb above the purely technological dimensions of the Internet and security.

It is by providing transparent and controllable security solutions and genuine universal know-how that the security market will achieve a level of maturity that corresponds to the stakes. It is by knowing "who controls security," and by being aware of all the relevant risks, that it will be possible to establish the appropriate level of confidence between the different providers and customers of information and communication technologies. Through this the technological world will contribute to the construction of an inclusive information society, helping personal and economic development. Thereby cybersecurity will become a cornerstone of the success of the Internet.

1.3 Supporting and developing the digital society

The evolution of a specific society

The transformation of societies into an information society, a process made possible by the integration of new technologies in every sphere of activity and every type of infrastructure, increases the dependence of individuals, organizations, and countries on information systems and networks. This is a major source of risk, which must be treated as a security risk. In addition, there is an increasing awareness of the importance of mastering operational computer risks, with the growing utilization of new technologies, the existence of a global information technology infrastructure, and the emergence of new risks generated by cyberattacks.

There is a danger that individual or small enterprises, as well as developing countries, in attempting to join the information society, will put too few of their limited resources into security infrastructure. 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.

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, etc.). It is not a matter of technology alone. 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.

An exclusive approach

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

Given the financial, material and human resources that countries have invested in creating their information and telecommunication infrastructure, they must ensure that the infrastructure is secure, well managed, and controlled.

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 ethics needed to handle security and meet the expectations and needs of society (Figure 1.6).

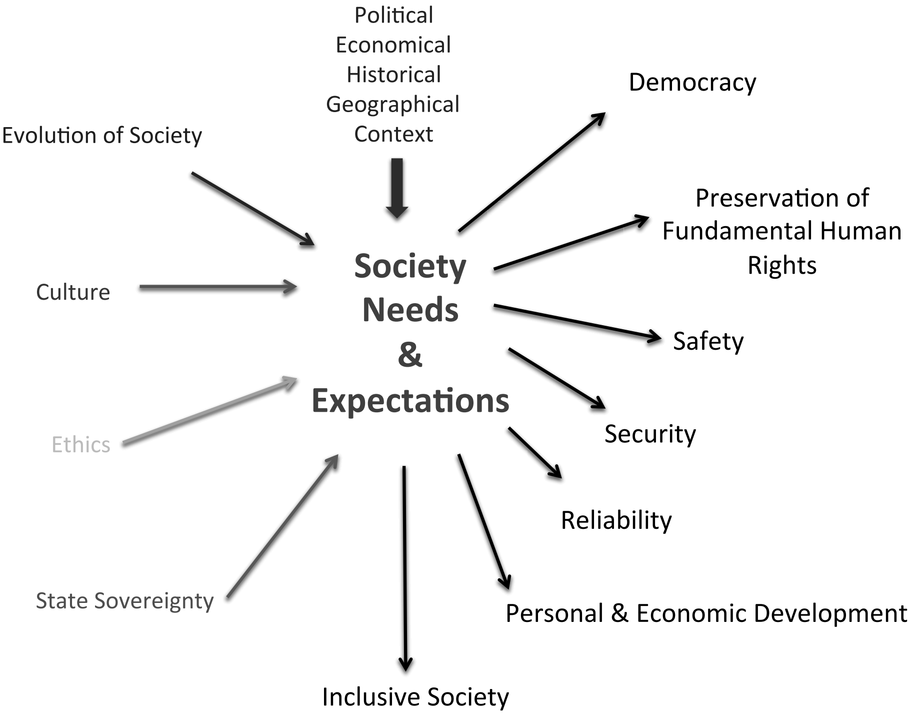


Figure 1.6 Some specific constraints and requirements to support the digital and networked society.

Currently, there are a host of partial regulations from a variety of organizations regarding communication media and the freedom to send and receive messages. These organizations include, for example, the United Nations (UN), the International Telecommunication Union (ITU), UNESCO (United Nations Educational, Scientific and Cultural Organisation), the Organisation for Economic Co-operation and Development (OECD), or the Council of Europe. Developments in information and communication technologies and the way people use them have outpaced the regulations governing them. Therefore, there is a need for an appropriate legal framework to be instituted to address such issues as the extra-territorial nature of the Internet, the problems of responsibility, and the protection of privacy and of property rights, to give only a few examples. Technological evolution needs to be paralleled by an evolution of the social, political and legal orders. This cursory examination already provides an idea of the importance of the challenges created by the information age, the crucial role of telecommunications in meeting them, and the importance of dealing with security issues before they hinder development.

1.4 Cybersecurity expectations

A major issue to consider: absolute security cannot exist

An emailing system does not offer any security services. Data transmitted in "clear," unencrypted, can easily be intercepted. Messages can therefore be read, modified or destroyed. There is no guarantee of the confidentiality or integrity of the data transmitted, no guarantee of the origins of a message or of its receipt. It has long been recommended not to transmit any important or secret information through email. At another level, access to web servers is mostly achieved without any mutual authentication mechanism between the client and the server that would allow the Internet user to guarantee that he has correctly been put in relation with a specific server, that the website is the original one, or that the data are correct. Furthermore, when we download data, there is no way to know if it contains any malicious additional content (such as a virus). As a general rule, all software, services or data that we can download for free (when normally it would be paid for) should be considered as containing tools that could allow the end-user's machine to be hacked. Everything that seems too good to be true will generally constitute bait for infecting a user's machine or stealing information. It falls to the user to decide the authenticity of the information, contacts or exchanges he has in cyberspace. It falls to him to determine what is true and what is false, knowing that tools for establishing integrity and authenticity are neither widespread nor reliable.

In addition, encrypting data in order to make them confidential also contributes to making them incomprehensible to people who do not possess the decoding key. Here security solutions that employ encrypting processes do exist. They can be used to make commercial or financial transaction data confidential, for example. Even the use of famously robust solutions cannot, however, guarantee that they cannot be broken, even though they do typically resist attacks better than other approaches. Trust in security solutions based on encryption can only be relative, to the extent that even the most robust mechanisms are implemented in environments that are, by definition, fragile. Furthermore, encrypting or decoding keys, stored in machines, can be stolen, and encryption solution providers do essentially control confidential data. In fact, security solutions need to be secured (Figure 1.7).

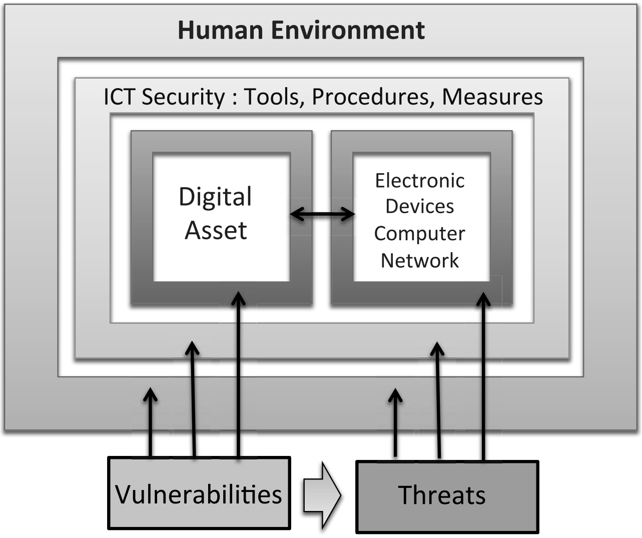

Human Environment
ICT Security : Tools, Procedures, Measures
Digital Asset
Electronic Devices Computer Network
Vulnerabilities
Threats

Figure 1.7 ICT security solutions are vulnerable and should be secured and reliable.

The objectives of availability, reliability, confidentiality, and integrity confer a certain quality to electronic exchanges and are reliable measures for the user of cyberservices. So ICT security is necessary for the success of the Internet. Without descending into paranoia, we should remind ourselves that, as with computing solutions, security solutions are fallible. They can be bypassed or weakened. It is not simply because a security measure has been implemented (*firewall*, antivirus, encryption, etc.) that the computer is protected against every possible kind of attack. In general, if the measured is well designed, managed and used, it reinforces the security of the system. By analogy, illegally entering a house with a reinforced door is much harder than getting into one with a wooden door. However, a reinforced door, even a very resistant one, will be useless if the thief can enter through a window. The reinforced door will stop the petty thief who prefers easy targets, but it will not stop the motivated thief from finding an efficient way to achieve his objectives.

Thus security solutions respond to particular situations at a specific moment by, mostly, displacing the problem of and responsibility for security. Many solutions quickly become useless because methods of attack and criminal know-how are evolving. Cybersecurity has to develop the confidence that citizens have in their governments and in the commercial entities on which they depend and with whom they interact. Applying efficient and coherent measures that allow for the management of computing risk – or that transform it into an opportunity for controlling security – has become fundamental both for state sovereignty and business competitiveness.

The demand for efficient and effective cybersecurity measures

Whether under the name of information security, computer and network security, or cybersecurity, this subject impacts the security of the digital and cultural wealth of people, organizations, and countries (Figure 1.8). It is a social issue as well as one of economics and public policy. The challenges involved are complex, and meeting them requires the political will to devise and implement an overall strategy for the development of digital infrastructures and services that includes a coherent, effective, verifiable, and manageable cybersecurity strategy. The cybersecurity strategy must be part of a multidisciplinary approach, with solutions in place at the educational, legal, management, and technical levels. A strong response to the human, legal, economic, and technological dimensions of digital infrastructure security needs builds confidence and generates economic growth that benefits all of society.

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

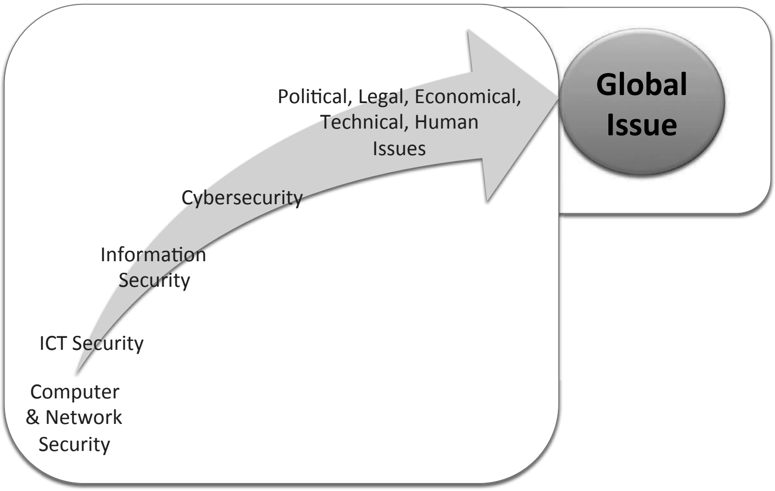


Figure 1.8 Cybersecurity for individuals, organizations and countries

The following are required if activities based on information processing grow, thereby helping to narrow the digital divide:

- reliable and secure information infrastructures with guaranteed accessibility, availability, dependability and continuity of services;
- policies that create trust;
- an appropriate legal framework;
- judiciary and police authorities conversant with new technologies and able to cooperate with their counterparts in other countries;
- information risk and security management tools;
- security implementation tools that will foster confidence in the applications, the services provided (e-business, e-finance, e-health, e-government, e-voting, etc.), and in the procedures set up to protect human rights, especially privacy.

The goal of cybersecurity is to help protect a given institution's assets and resources in organizational, human, financial, technical, and information terms.

The ultimate objective is to ensure that no lasting harm is done to the organization. This consists of the following actions:

- reducing the likelihood that a threat materializes;
- limiting the damage or malfunction resulting from an incident;
- ensuring that, following an incident, normal operations can be restored within an acceptable timeframe and at an acceptable cost.

The cybersecurity process involves the whole of society; every individual is effected by its implementation. It can be strengthened by developing both a cyber code of conduct and a genuine security policy that stipulates standards for cybersecurity users, entities, partners and providers to meet.

1.5 Summary

In today's world, widespread system interconnection increasingly links infrastructures, and expands dependence on digital technologies – and the threats and risks that accompany these developments. It is necessary for individuals, organizations and countries to take steps, adopt procedures, and acquire tools:

- to improve the way that technological and cyber-risks are managed; and
- to improve the way that cybercrime is handled at national and international levels.

The struggles to maintain information and technological risk at an acceptable level and to conquer cybercrime are at the heart of the challenges facing us in the twenty-first century. We need a comprehensive global approach to cybersecurity. It is not enough to set up points of access to telecommunication networks. It is necessary to deploy ICT infrastructures and e-services that are reliable, maintainable, robust and secure, while respecting basic human rights and state sovereignty. 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.

Dealing with the complex, multifaceted cybersecurity problems raised by a networked society can be daunting. The potential repercussions and impact on the operation of organizations and countries are devastating. The ability to provide security for information, processes, computer systems, and ICT infrastructure is crucial to the success of a given economy. It is essential to ensure that cybersecurity does not become another dividing line between the haves and the have-nots.

1.6 Exercises

1. For a state, what are the new risks introduced by an economy, based on the use of information technologies and telecommunications infrastructures that are interconnected at a global level?

2. Societies are increasingly becoming information and digital societies in which the majority of services are provided or enabled through information and telecommunications technologies. What are the principal impacts of this?
3. Based on the answers to questions 1 and 2, what are the major challenges to be addressed by the public authorities?
4. Why is it utopian to think that states, independently of each other, could be able to address the challenges raised by the information revolution?
5. Why can the Internet be considered to be a critical infrastructure?
6. What is meant by "an inclusive information society"?
7. Why is cybersecurity at the heart of the debates around the development of the information society?
8. What is the relationship between cybercriminality and cybersecurity?
9. Why does cybersecurity need to be considered from an interdisciplinary perspective?
10. Why is cybercriminality a problem for society?

Chapter 2

Cyberspace and Internet: a New Paradigm for Crime and Conflicts

2.1 Understanding the context

Because the Internet enables the rapid transmission of data, regardless of both the distance between the source and the destination end-points and their localisations around the globe, cyberspace has extended and modified the temporal and geographical borders to which we have been accustomed. This has upset our habits, imposed new ways of functioning, and created new societal values; at the same time, it has created unprecedented changes in communications and introduced a new digital order. The size of the changes introduced by the urbanization of digital technologies can be termed an "information revolution." The dematerialization of information, transactions, and services has permitted new forms of organisations and exchanges and innovative forms of activities – both legal and illegal. Criminality, organized or not, has widely adopted ICT in order to improve efficiency, leading to harmful consequences for society.

Some of those in search of profit or power have quite naturally utilised the Internet and cyberspace in order to reach their objectives. Computing technologies and telecommunications are the targets of malevolence, and they provide the means of committing illicit actions (Figure 2.1). These technologies are at once the platforms for, and means of, committing both new offences and traditional ones, especially offences related to financial or business activities.

From the headlines

Internet Poker Companies Indicted for Fraud, Money Laundering[1]

Internet Escort Services Firms Charged with Money Laundering/Agree to Fine and Forfeiture Totalling $6.4 Million[2]

TomorrowNow, Inc., Sentenced on Computer Intrusion and Copyright Infringement Charges/Company Agrees to Pay $20 Million Fine[3]

Former IT Technician Sentenced to Jail for Computer Intrusion[4]

Florida Man Arrested in "Operation Hackerazzi" for Targeting Celebrities with Computer Intrusion, Wiretapping, and Identity Theft[5]

An example of this would be unauthorized access via the Internet to a bank's information systems in order to steal or modify financial data; in this scenario, computing and network resources form both the means of the crime and, in the form of the bank's systems and financial data, the targets. Incidentally, from a legal perspective it can be hard to determine whether such activities constitute cybercrime or financial crime. In any case, more and more economic crime is linked to cybercrime, and cybercrime, more often than not, involves economic crime. As a means of committing and coordinating criminal activities, the Internet is a hugely efficient and robust communication tool that facilitates many activities, including illegal ones.

[1] Source: ABCNews, 15 April 2011.
http://abcnews.go.com/Technology/internet-poker-companies-indicted-fraud-money-laundering/story?id=13386037#.TwQapU-E9aQ

[2] Source: The Federal Bureau of Investigation – Philadelphia division. U.S. Attorney's Office. November 1, 2011 – Middle District of Pennsylvania (717) 221-4482
http://www.fbi.gov/philadelphia/press-releases/2011/internet-escort-services-firms-charged-with-money-laundering

[3] Source: The Federal Bureau of Investigation – San Francisco. Division U.S. Attorney's Office. September 14, 2011 – Northern District of California (415) 436-7200
http://www.fbi.gov/sanfrancisco/press-releases/2011/tomorrownow-inc.-sentenced-on-computer-intrusion-and-copyright-infringement-charges

[4] Source: The Federal Bureau of Investigation – Tampa Division – U.S. Attorney's Office. December 7, 2010 – Middle District of Florida (813) 274-6000
http://www.fbi.gov/tampa/press-releases/2010/ta120710.htm

[5] Source: The Federal Bureau of Investigation – Los Angeles Division. FBI Los Angeles. October 12, 2011. Public Affairs Specialist Laura Eimiller (310) 996-3343
http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft

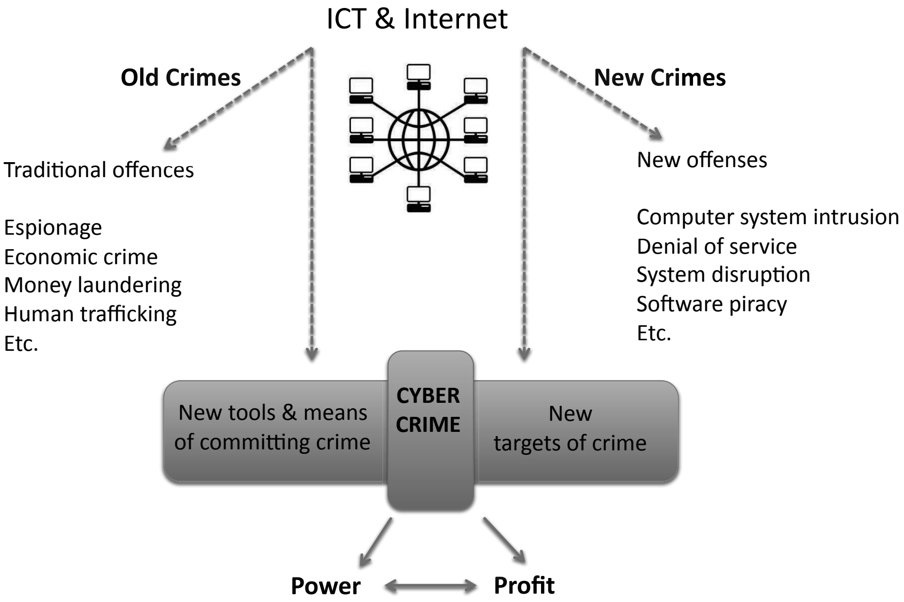


Figure 2.1 ICT as a tool and means of committing crime.

Cybercrime is defined as any criminal activity performed through cyberspace or the Internet. By extension, it includes every form of digital malevolence carried out using digital technologies, electronic devices, and telecommunications networks (such as telephones, smart cards, and ATMs, for example). *Criminal activity* includes activities that are illegal, illicit, irregular, or against the law. Cybercrime thus covers a wide range of activities; most currently existing illegal acts can be performed on or over the Internet.

The end result and the context of the original creation of the Internet have evolved progressively. The changes that were implemented have created a new communication paradigm that can be summarised by "Communicate anywhere, anytime, with anyone." The notion of "anyone" does not only encompass children, old people, Mr. and Mrs. Everyone and professional people, but also individuals and groups with dishonest intentions (such as pedophiles, terrorists, criminals, delinquents, and professional swindlers). The Internet is used for private and professional purposes. E-services are both for entertainment and for doing business. This almost unlimited communication exposes every Internet user to different risks arising from criminal origins. The cyberproximity to criminality facilitates the meeting and the juxtaposition of two worlds that, until recently, had been relatively well compartmentalized: the worlds of bandits and non-bandits (Figure 2.2).

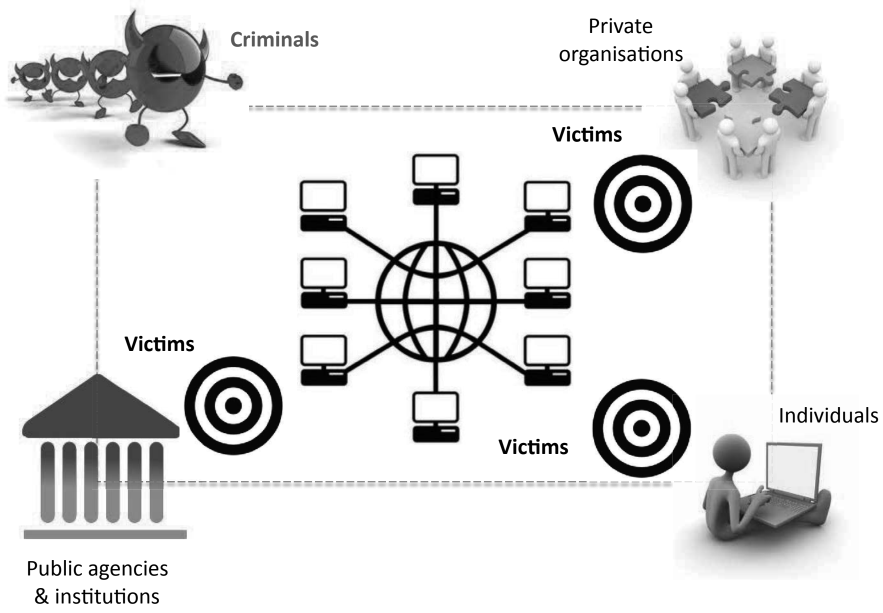


Figure 2.2 Cyberproximity to cybercrime.

From the field

Child Predators. The Online Threat Continues to Grow[6]
"It's an unfortunate fact of life that pedophiles are everywhere online," said Special Agent Greg Wing, who supervises a cyber squad in our Chicago Field Office. When a young person visits an online forum for a popular teen singer or actor, Wing said, "Parents can be reasonably certain that online predators will be there." It is believed that more than half a million pedophiles are online every day. Pedophiles go where children are. Before the Internet, that meant places such as amusement parks and zoos. Today, the virtual world makes it alarmingly simple for pedophiles – often pretending to be teens themselves – to make contact with young people.

The Internet and cyberspace can both be considered criminalized zones. Individuals and private or public institutions, due to their presence on the Internet, contribute to the extension of cybercriminality because they increase the number of potential attractive targets for cybercriminals.

[6] Source: The Federal Bureau of Investigation, 17 May 2011. http://www.fbi.gov/news/stories/2011/may/predators_051711/predators_051711

The Internet contributes to removing many commonly-recognised, natural or cultural boundaries to which we are accustomed, such as those between the young and less young, civilians and military personnel, the public and private spheres, leisure and professional activities, and legitimate and criminal acts.

Nowadays everyone uses – and sometimes misuses – the same kinds of information and communication technologies, the same Internet and shared cyberspace (Figure 2.3). Through cyberspace, the victims of criminality could be everyone, civilian and/or military, and any private or public institution.

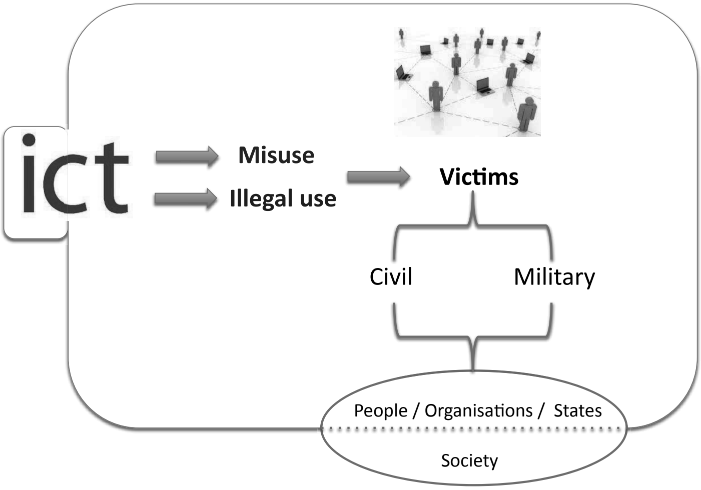


Figure 2.3 Internet: a remover of frontiers.

The Internet remains a complex and multiform environment that is in constant evolution. At the same time, it forms a tool for destabilization and criminal activities that contributes to the creation of a chaotic and hostile universe that can serve many kind of conflicts: those originated by individuals (civilians, recreational hackers, "hacktivists," ideologues, terrorists, criminals, mercenaries), by legal or illegal organizations (such as mafias and organized criminal groups), or by states (democratic or rogue states.)[7]

When referring to cybercriminals and cybercrime, the underlying assumption is always that the malevolent parties are non-state individuals or groups carrying out criminal actions across the Internet. The term *cyberconflict* is mostly linked to nation-states, and the term *cyberterrorism* is related to the use of cyberspace for terrorist purposes, as defined by national or international law.

[7] The question of knowing who could be a cybercriminal is addressed in Chapters 9 and 10.

When viewed in the widest sense, including the systems, networks, data and programs that make it up, the Internet can be considered as (Figure 2.4):

- a source and a means of wealth creation for criminals;
- a symbol to be destroyed for terrorists; or
- an entity and a means of destabilization and of waging economic and/or military war on businesses or states.[8]

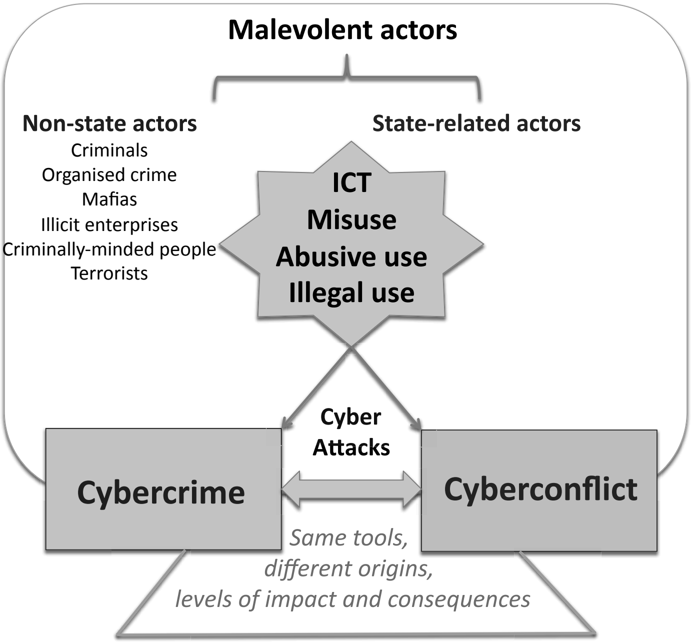


Figure 2.4 Different perceptions of the Internet.

2.2 The characteristics of cybercrimes

From the perspective of terminology

The root "cyber-" comes from the word *cybernetics* which was coined in French in 1834 to describe the "science of government," from the Greek *kubermêtiké*, the feminine of *kubermêtikos*, derived from *kubernan*, meaning "leading, steering." The term was introduced into the English scientific lexi-

[8] These aspects will be further developed in Chapters 4, 5, 6, 7 and 8.

con in 1948 by Norman Wiener, and this gave birth to cybernetics,[9] a science covering all the theories relative to the control, regulation and communication of human beings and machines. A cyborg[10] is a humanoid electronic organism.

The prefix cyber- has subsequently frequently been applied to defining automatic treatments made possible by computing techniques and telecommunications. It has become specific to telecoms and multimedia, especially related to the Internet. A cybernaut, then, from "cyber-" and "astronaut," is a person who moves, who "surfs" in cyberspace. Cyberspace is a space created by humans using Internet technologies[11] that permits the manipulation of information[12]. The term, and the domain, includes all the information resources that allow the emergence of a digital universe, creating a new kind of digital reality that was quickly dubbed *virtual reality*. Finally, a *cybercafé* is a café where customers can surf on the Internet thanks to the provision of personal computers and an underlying telecommunications infrastructure.

By adding the prefix "cyber-," which refers to activities performed on or through the Internet, new forms of wrong-doing can be identified – cybermalevolence, cyberviolence. They can be associated with classic (because of their age) crimes that are now being perpetrated across the Internet: cyberswindles, cyberfrauds, cyberextortion, cyberabuse, cyberspying, cybervandalism, cyberconflict, etc. New terms are regularly being coined to describe the performance of malicious acts across the Internet, with a common trend being that the prefix e- (for electronic) replaces "cyber-," as in e-trading and e-fraud, for example.

The common theme in this new vocabulary that is so closely tied in criminality is the idea of behaviour that exploits the characteristics of the Internet. The precise actions can be old-fashioned crimes facilitated by ICT technologies (for example, money laundering, financial fraud, economic crime, infringement of copyright), or new crimes that are now possible because of ICT technologies (for example, the theft or hacking of computers, the theft of digital data protected by intellectual property rights, or software piracy).

[9] *Cybernetics* – the science of communications and automatic control systems in both machines and living things (Oxford English Dictionary).

[10] *Cyborg* – a fictional or hypothetical person whose physical abilities are extended beyond normal human limitations by mechanical elements built into the body (Oxford English Dictionary).

[11] The Dictionary of military and associated terms of the US Dept. of Defence, defines *cyberspace* as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, an embedded processors and controllers." Source: CJCS CM-0363-08 – http://www.dtic.mil/doctrine/dod_dictionary/

[12] Information manipulation includes the creation, the transmission, the processing, the storage and the deletion of information.

Cybercrime, crime assisted by a computer, is regarded as a high technology crime because it requires, at least in principle, a certain level of technical competence and technological tools in order to be perpetrated. It is also described as electronic crime. When cybercriminals are educated people committing crimes without metaphorically getting their hands dirty, these activities are also often referred to as white-collar crimes.

From a legal perspective

A crime is any prohibited action; laws must exist to define what is and is not legal. The notion of cybercrime is still not defined precisely as a result of multiple definitions, interpretations and national jurisdictions. Committing illegal acts in or via cyberspace could be characterized by the fact that the criminal, using the Internet, is hidden behind a screen and is acting remotely for criminal purposes, as defined by national or international law.

One of the oldest definitions of a computer related crime was given in 1983 by the Organisation for Economic Co-operation and Development. The OECD defined a computer related crime as any illegal, unethical, or unauthorized behaviour involving the transmission or automatic processing of data. All information and communication technologies and digital devices can potentially be involved in a computer related crime; in this context we can cite mobile and wireless technologies, cellular networks, telecom infrastructures, servers, telephones, smart cards, ATM, nanotechnologies, captors, control centres, GPS systems, DVD readers, multimedia platforms, etc.). They can be used to commit or to be the target of crimes. A computer crime is a crime where the computer system can be either

- the object or the target of the crime (true computer crime);
- the means of committing the crime. The computer is the instrument of the crime (computer related crime); or
- both.

A computer crime is a crime connected with digital technology. Cybercrime is a form of computer-related crime committed using Internet technology; it covers all crimes committed in cyberspace.

Computer-related crimes are variously called: technological crimes, high-technology crimes (high tech crimes), computer- and Internet-related crimes, computer-assisted crimes (as in fraud or money laundering), computer-focused crimes (as in website defacement), digital crimes, or electronic crimes (e-crimes) (Figure 2.5). Cybercrime refers to a broad range of illegal activities

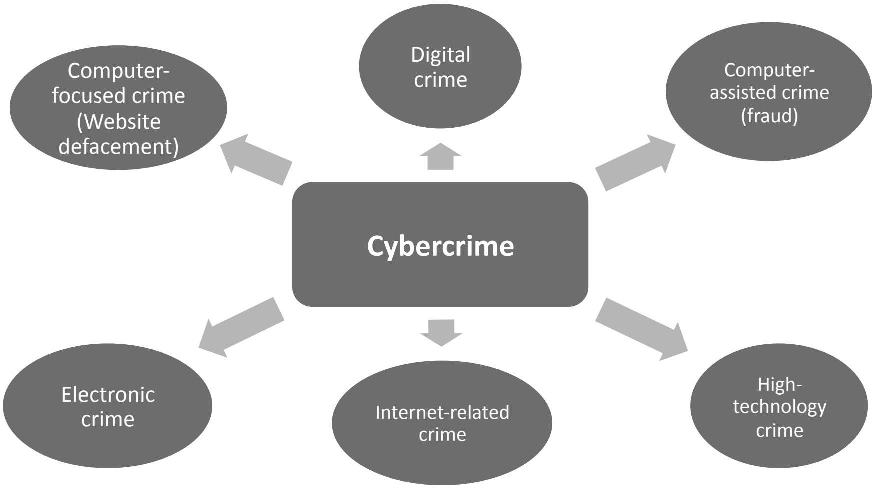


Figure 2.5 Cybercrime, a generic term for multiple illegal activities that involve ICT.

perpetrated through cyberspace by means of information and communication technologies (ICT).

The *Organized Crime Situation Report* of 2005, published by the Council of Europe,[13] divides cybercrime into the following types of offences (Figure 2.6):

- Offences against the 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 fishing), computer espionage, computer sabotage and extortion.
- 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.

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

- 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 to be criminalized under the 2001 Convention on Cybercrime (ETS 185) and the Additional Protocol to the Convention on Cybercrime. This additional protocol concerns the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189).[14]

This report documents the many different facets of cybercrime, making the distinction between (i) crimes against persons; (ii) crimes against assets; and (iii) crimes against institutions and states.

The Convention is the first international instrument that provides a framwork for harmonizing cybercrime legislation across countries.

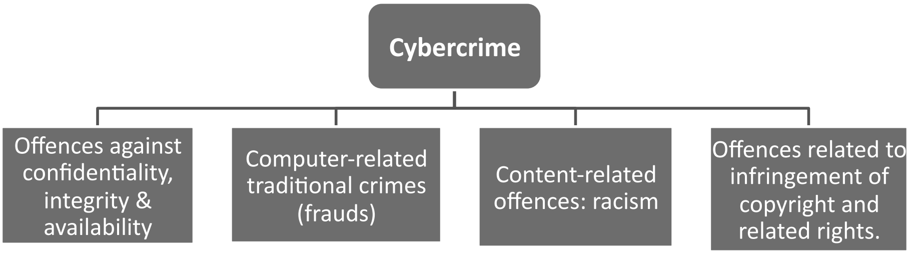

Cybercrime
Offences against confidentiality, integrity & availability
Computer-related traditional crimes (frauds)
Content-related offences: racism
Offences related to infringement of copyright and related rights.

Figure 2.6 Types of offences as identified by *Organized Crime Situation Report* 2005 of the Council of Europe.

The fact that criminality and delinquency is a matter of penal law for individual states has caused the creation of multiple definitions, characteristics, and typologies of cybercrime, all of which vary from one state to another. The Convention on Cybercrime from the Council of Europe, without specifying explicitly the term cybercrime, defines the infractions that are relevant to it. As summarised in its preamble, the Convention addresses "[…] the necessity to lead, in priority, a common penal policy destined to protect the society from criminality in cyberspace, especially through the adoption of an appropriate legislature and through the improvement of the international cooperation; […] preoccupied by the risk that data processing networks and electronic information may be used also in order to commit penal infractions and that proof of these infractions are kept and transmitted through these networks […]." The

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

preamble of the convention delimits the boundary of cybercrime by placing its measures in the context of protection of fundamental rights, which includes the protection of personal data and the protection of people against the automated processing of personal data: “Keeping in spirit the necessity to warrant an adequate equality between interests of the repressive action and respect of human rights, such as warranted in the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (1950), in the International Covenant on Civil and Political Rights of the United Nations (1966), and other international conventions regarding human rights which reaffirms the right of not being harmed for one’s opinions, freedom of speech, freedom to search, obtain, and communicate information and ideas of all kinds, without consideration of any borderline and the right of the respect of private life […].” In addition to the different offences listed, the Convention puts the accent on “the necessity of a cooperation between States and the private industry in fight against cybercrime, and the need to protect legitimate interests in using and developing information technologies; […] a fast and efficient international penal cooperation; […] in order to facilitate the detection, investigation and prosecution, on a national and international level.”[15]

Depending on the role played by information and communication technologies, other distinctions can be made based on the fact that:

- A crime can be committed by other means (such as classical, “old” crimes), criminals then take advantage of ICT to optimize their criminal performance. ICT can be considered as new criminal tools.
- A crime can be committed only by means of ICT, which means that ICT creates new criminal opportunities. The cyberspace can then be considered as an extension of the criminal world. The technologies combine to create new tools that can make new crimes possible.

There is no unique or agreed-upon definition of cybercrime, and some authors use existing categories drawn from criminal laws into which their cyber-counterparts can be placed, and then subdivide cybercrime into different categories according to the object or target of the offence, for example:

- Cybertrespass: crossing boundaries into other people’s property and/or causing damage (e.g. hacking, defacement, virus), “crime against property”;
- Cyberdeception and theft: stealing money or property (e.g. intellectual property violations, piracy), “crime against property”;

[15] Source: Council of Europe – STCE no 185 – Budapest 23.XI.2001.

- Cyberpornography: breaching laws on obscenity and decency, “crime against morality”;
- Cyberviolence: causing psychological harm to or inciting physical harm against others, thereby breaching laws relating to the protection of the person (e.g. hate speech, stalking), “crime against the person”;
- “Cybercrime against the state”: breaching laws protecting the integrity of the nation and its infrastructures.

Regardless of the legal context relating to the definition of a crime, and although the Internet is considered to be a global and international space, each Internet user is situated in a geographical and temporal space where everything that’s illegal *offline* is also illegal *online*. Furthermore, the user’s behaviour is also influenced by moral and ethical practices that reflect the values of his society.

From an ethical point of view

In reality cybercrime can refer not only to illegal acts but also to deviant behaviour. A crime is any action or omission prohibited by law and punished by the State. So, criminal laws must exist to refer to illegal acts, and laws can vary from one nation to another. Dealing with cybercrime issues at the international level is a real problem because many different national legal systems exist.

The boundaries between *deviant* and *illegal* are dependent on, and influenced by, social context. Deviance is an act that breaches informal social norms and rules and is thus considered undesirable or objectionable. A deviant behaviour is always linked to ethical or moral points of view. These morals vary from one culture to another and from one period to another. An act can be deviant without being identified as illegal by the law. In fact, some acts may not be illegal, but rather deviant – from a particular point of view. Behaviours that are identified as deviant with regard to the morals, standards, ethics, or habits of a particular culture can sometimes be relevant to cybercrime (Figure 2.7). The definition of what is legal and what is not depends on the applicable law in a considered state. So, in a global, international context, it is necessary to focus on illegal activities that are widely recognized as crimes in different countries and share a common definition, without taking into account deviant activities. As an example, we can see notable differences in the definition of the age of consent. This is the age at which an individual can have a sexual relationship with somebody of his choice without this being illegal.

The sexual majority age varies from country to country; currently it is set at sixteen in Switzerland, fifteen in France, and thirteen in Spain. Thus, in this example, what is illegal in Switzerland is not illegal in Spain. In a similar way, some cyberactivities are considered offences in some countries and not in others.

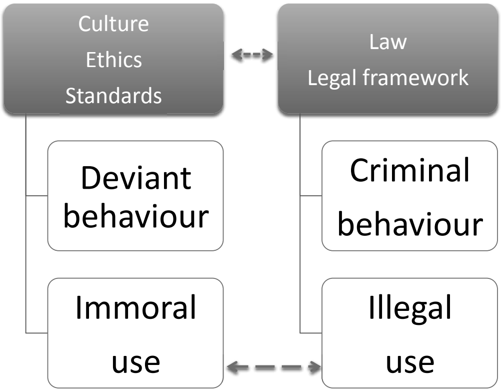


Figure 2.7 Deviant and criminal behaviour through the Internet.

From a technological point of view

Whatever terminology is employed, no matter what legal framework cybercrime is related to, cybercrime covers the whole range of possible crimes committed through ICT technologies and cyberspace. These are typically sophisticated and sometimes crimes that can be committed by:

- force: intrusion into a system (hacking), breaking security mechanisms;
- fraud: identity theft, usurpation of connection parameters;
- delusion: mainly by diversion of the normal means of functioning of ICTs (“scams” and “cons”).[16]

A cybercrime can be large-scale and simultaneously affect a considerable number of targets (cyberepidemic). It can have almost instantaneous or delayed effects. It can be committed far from the place where the harm is done.

[16] See chapter 8 for more details.

2.3 The Internet: empowering criminals

Very desirable and invaluable assets

Nowadays, information makes up the digital assets of individuals, organizations and States. The dematerialised assets of our new civilization take the form of the digital information processed and stored by computers and transmitted through telecommunications networks. So information and the technologies that support them have to be considered as important strategic and valuable resources. This information has an intrinsic value that can be the object of envy and illegal misappropriation. The same is true for the technologies (computers, networks, programs) and infrastructures that support this information and make it available (Figure 2.8).

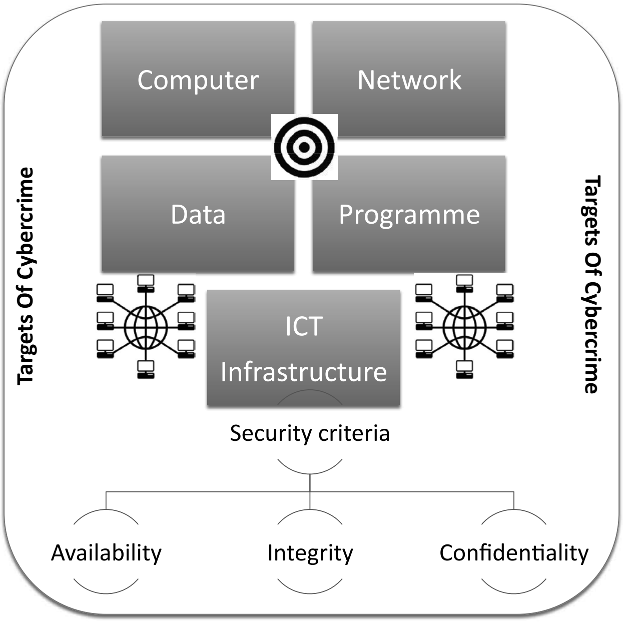


Figure 2.8 The principal targets of cybercriminal intentions.

A computer system is not the only target of criminal intent, neither is it necessarily the end point of a cyberattack; more often it is the related software or data that are targeted. For example, an Internet user's personal computer does not necessarily possess any great market value, but the fact that it can serve as a relay for carrying out attacks on other systems confers upon it an incalculable value that is not usually obvious to its owner.

From the Press

Financial Records of Millions At Risk After Computershare Insider Copies Data To USB... Then Loses The USB.[17]

Facebook Tools to Help Data Thieves. New feature that allows Facebook apps to collect user addresses and cell phone numbers could easily be used by scammers.[18]

Norway Cyber Attack Targets Country's Oil, Gas Systems
Norway's National Security Authority (NSM) on Friday confirmed that systems associated with the country's oil, gas, and energy sectors were hit with a cyber attack, resulting in a loss of sensitive information.[19]

The same is true of personal data that, at first sight, might not seem to have any market value. But these data can be used to perpetrate malevolent acts. For example, in everyday life, the full name and address of an individual are widely known and not especially protected. Indeed, this information can be found in a phonebook and on a mailbox, and many entities and people know them (postman, employer, insurer, neighbours, etc.). Most of the time, this does not cause any problems. When we meet somebody, he introduces himself and provides this information of his own free will. When associated with a face – a real person – these data allow the establishment of a direct link between a name and an individual, hence his identification and recognition. It is hard for a wrongdoer to pretend to be somebody else without changing the picture on an ID card or transforming his appearance to look physically like the person.

On the Internet it is different because these same elements of data are not directly linked to a physical person. These data are often easily accessible. Criminals have learned how to appropriate these data to commit illicit acts in the name of the victim whose identity has been stolen (the idea of impersonation). If the acts lead to investigations with a view to prosecution, it will often be virtually impossible to identify the real guilty parties; the victim of the impersonation will automatically appear responsible.

Personal data such as names, passwords, connection parameters, bank account numbers, and social security numbers are frequently searched for

[17] Source: threatpost. The Kaspersky Lab security News Service. Paul Roberts. November 8, 2011, https://threatpost.com/en_us/blogs/financial-records-millions-risk-after-computershare-insider-copies-data-usbthen-loses-usb-1108

[18] Source: Infoworld. Robert Lemos. 17 January 2011. http://www.infoworld.com/t/data-security/facebook-tools-help-data-thieves-711

[19] Source: PCMag. Chloe Albanesius. 18 November 2011. http://www.pcmag.com/article2/0,2817,2396611,00.asp

and hold great value. They can be obtained by deceiving the user. Frequently, fraudsters pose as entities known to the Internet user, such as a bank or a manager of his messaging service, and ask him – always with some credible justification – to communicate his personal data by phone, through a website or by mail. This type of activity, consisting of manipulating people in order to lead them to take specific actions or to reveal confidential information, is a kind of confidence trick known as "social engineering." Taken in by the apparent good faith of the request, the user provides voluntarily the kind of information that will later be exploited to harm him. It is true that the principles of this kind of fraud have existed for many years and do not require great technical skills; however, the harvesting, storage, processing and subsequent reuse of the data, particularly if gathered by sniffing or interception, do require a level of technical skills.

A real case of identity theft from the press

> […] cases of a five-month-old boy with a bankruptcy on his credit file and a 17-year-old girl with over $725,000 in debt. Both had been victims of identity theft […] The culprits often are relatives with access to personal information. But a more daunting group often pulls off the attack: organized-crime rings. The rings typically sell the data to people who open lines of credit or apply for cellphone accounts, or to illegal immigrants trying to get working papers. Evidence of the fraud can emerge in the mail in the form of a credit offer or collections notice addressed to a child. […] The theft can cause long-lasting damage and can come as a shock right when a child is ready to become more financially independent, such as when a child is preparing for college and applying for financial assistance. […] Nineteen-year-old H. B. of Somerset, N.J., got a rude awakening when she applied for her first bank card before going to college: She discovered roughly $16,000 worth of debt attributed to her Social Security number. The first fraudulent credit account was registered years before she was born… for a criminal, a child's identity – including that fresh Social Security number you often write down on health forms and school documents – […] Experts also warn against broadcasting children's birthdays and names on Facebook, Twitter and other social-media services—and urge people to come up with strong passwords for email, shopping and social networking […].[20]

A real underground business has grown up around the market for the sale or rent of technical tools (cyberweapons), particularly in the domains of mal-

[20] Source: Wall Street Journal, 27 August 2011. M. J Randall, D. Lim. http://online.wsj.com/article/SB10001424053111904292504576484731212444942.html

ware and zombie computers (botnets) that simplify the carrying out of cybercrimes. The market also extends to the provision of personal and identification data, such as email addresses, connection information and banking data[21].

Internet can facilitate criminal activities

The specifications and means of operation of the various Internet technologies are public and well known. The same is true of their technological vulnerabilities. These are usually revealed to the public through various dedicated websites or diffusion lists, such as the information notes on system vulnerabilities regularly published by organisms such as CERT (*Computer Emergency Response Team – Carnegie Mellon University*).[22] By these means everyone can be informed about existing and newly discovered vulnerabilities. The administrators of affected systems can then apply this information to reinforce system security by implementing security patches. At the same time, those of a criminal or malicious disposition can take these vulnerabilities into account when designing attacks that exploit them.

A market exists for information on vulnerabilities and related attack software and methodologies. On the Internet, everything can be bought or sold, and this applies to the discovery of vulnerabilities. Such knowledge can be auctioned off or sold before the necessary security responses have been developed and published and the relevant patches installed.

News from the web

> *Cyber Attack Toolkits Dominate the Internet Threat Landscape*
> […] Criminals who don’t have the knowledge or skills to develop malware on their own are turning to someone who does. These attack toolkits allow the purchasers to contribute to the global mess of malware and cybercrime. Attack toolkits are increasingly available to an unskilled black market that is eager to participate in the speedy spread of malware. […] One particular toolkit called Zeus, which aims at stealing bank account credentials, accounted for 65 percent of all advertisements for the sale of kits on underground economy servers observed by Symantec. In September 2010, the FBI revealed that a ring of cybercriminals was arrested for allegedly using Zeus to steal more than $70 million from online banking and trading accounts over an 18-month period. […] The widespread availability of attack kits has resulted in a much more

[21] Tools used in cybercrime are described in Chapter 8.

[22] http://www.cert.org/certcc.html

> diverse pool of cybercriminals. Instead of being a club exclusive to computer programmers, newcomers don't even need to know how to write a line of code – they just need the right amount of money. […] The people who buy these toolkits have found an easy way to get money and do so despite wreaking havoc for innocent users. Cybercrime already causes enough headaches, but now toolkits have made it possible for even more criminals to get in on the action.[23]

The individual who discovers a new vulnerability has the choice of selling it to the highest bidder, who is not always the developer of the product or service in question. Frequently the criminal world knows of vulnerabilities and the ways to exploit them before computer professionals do. The market for attack software and kits is similarly thriving. However, it would be wrong to think that this market only interests potential wrongdoers. Some commercial organizations, governmental agencies, and individuals do buy this kind of product – usually undercover – for example, to carry out spying operations.

A zero-day vulnerability is a new vulnerability from which no security patch yet exists. At the time of writing, the price of such knowledge on the underground market could climb as high as U.S. $200,000. Such discoveries are important and can be extremely valuable. By way of example, the Stuxnet worm (discovered in July 2010) that affected SCADA systems in nuclear plants in Iran exploited four zero-day vulnerabilities.[24]

From the press

> Stuxnet is the name given to a computer worm, or malicious computer program, that began to spread in mid-2009. It may the most sophisticated cyberweapon ever deployed. […] Stuxnet turned up in industrial programs around the world. But experts dissecting it soon determined that it had been precisely calibrated in a way that would send nuclear centrifuges wildly out of control, adding to suspicions that it was meant to sabotage Iran's nuclear program.[25]

[23] Source: Marc Fossi, Manager of Development, Symantec Security Response http://www.infosectoday.com/Articles/Cyber_Attack_Toolkits.htm

[24] More information related to Stuxnet worm and attack mode operandi can be found at: *www.symantec.com/.../w32_**stuxnet**_dossier.pdf*

[25] Source: The *New York Times*. Stuxnet. Updated, 15 January 2011. http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html

Sources of Internet weaknesses

The criminal world has embraced the Internet, which has provided an extension of its scope and new possibilities for profitable activities. However, the Internet can also fall victim to natural catastrophes (such as earthquakes and floods) or be affected by errors. Such incidents can provoke negative consequences with serious impacts that are as damaging to society as simple criminality. That this three-way origin of problems can lead to issues with the availability, integrity, robustness, reliability, or resilience of the Internet needs to be taken into account when securing information and communication systems that are connected to the Internet. The number and origin of the weaknesses that affect the Internet, and its points of vulnerability, are many and various. Figure 2.9 identifies the main sources of problems for an Internet infrastructure. These include natural disasters, errors and malevolence.

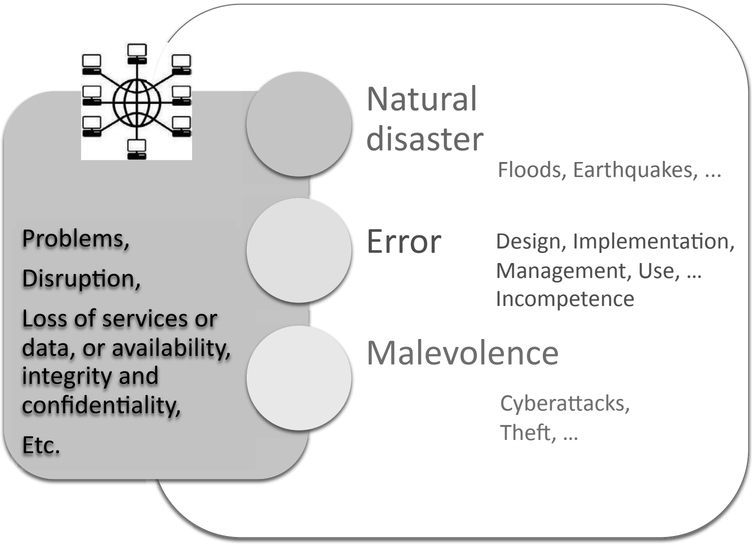

Problems,
Disruption,
Loss of services or data, or availability, integrity and confidentiality,
Etc.
Natural disaster
Floods, Earthquakes, ...
Error
Design, Implementation, Management, Use, ...
Incompetence
Malevolence
Cyberattacks, Theft, ...

Figure 2.9 The Internet and its many sources of problems.

Natural disasters

Natural disasters, such as floods, fires, storms and earthquakes, can affect ICT resources if they are not well protected. Some types of disaster are reasonably predictable, others not; undersea cable infrastructures, for example, are obviously vulnerable to earthquakes or tsunamis. There have been several natural events that have affected the availability of the inter-continental communications infrastructure in different parts of the world; one example of this would be that in August 2009, eight submarine cables were cut by an earthquake of magnitude 6.7 that had hit the east cost of Taiwan, in relation with the previous spread of Typhoon Morakot.[26]

News from the web

China-US Cable Network (China-US CN, or CUCN) suffered its second cable cut off the coast of China within a month. This cable cut broke down most of the Internet bandwidth linking the U.S. and China. The break occured at 21:13 on March, 9, 2001, at 123 Km away from Chongming Cable Landing Station, where the cable was buried under 32 m of sea level. The full capacity of the cable has been disrupted in what is believed to have been an accident caused by a fishing boat dropping anchor. The cable can carry as much as 80 Gbps (bits per second) of data and is one of the major links between China and the U.S., where a preponderance of the world's Web servers are located.[27]

Moreover, cable thefts are also a reality, and these can have the same devastating consequences on the overall operational mode of the Internet when international connectivity is required, for example to support international financial transactions. The availability, reliability, resilience and robustness of the Global Undersea Communications Cable Infrastructure (GUCCI) are critical requirements that need to be satisfied by appropriate measures in order to have a true global and international Internet with dependable international communications capabilities. Satellite communications cannot support either the traffic or the bandwidth capacity that are provided by intercontinental submarine cables.

Data centres will always be at risk from natural disasters. In particular, fire is a permanent threat that could damage the physical environments in which computers and communications devices and energy supply components are hosted, and potentially render them inoperable. Physical and environmental security is thus very important for ICT security.

[26] http://submarinenetworks.com/news/cables-cut-by-taiwan-earthquake-and-typhoon-morakot

[27] Source: http://submarinenetworks.com/systems/trans-pacific/china-us-cn/china-us-cable-break-down-internet

Errors and misuses

Errors are human failings and generally unintentional. Among the possibilities, for example, are errors relating to:

- software design, development or implementation;
- defective strategic management and risk analysis;
- bad specification of policies;
- ineffective system administration and operational management;
- faulty uses of a system or a service; or
- the understanding of a situation or a risk assessment;

The causes of errors can be diverse: an absence of training or information, incompetence, fatigue, a stressful working environment, a moment of inattention, or misconfiguration. An error that has been identified, but then is repeated because no remedial action has been undertaken, is a failing. Intentional errors should be considered to be malicious actions. Unwanted cyber-events could have an accidental or deliberate origin, and these would require a specific analysis in order to understand why they occurred, what their impacts were, and how to avoid them or to mitigate their negative consequences.

Misuse of Internet at work for personal matters, such as downloading software, songs or films, uploading photos, online shopping, online trading, chatting with friends, personal email, surfing on pornographic sites, exchanging adult content, gaming, etc., consume the users' time and the employers' ICT resources and could also lead to serious security breakdowns by violating the company's security policy rules and by introducing malware in the information system of the company.

Malevolence

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 and data and resource theft, modification, and destruction. Criminals exploit both the characteristics of how the Internet works and its vulnerabilities and points of weakness to carry out their business. A lack of control over the configurations of interconnected systems – hardware and software – can be exploited to commit ICT crimes, as can the known vulnerabilities of these systems and weaknesses in their administration. Furthermore, network administration tools, such as monitoring or remote configuration tools, can be used with malicious intent.[28] Figure 2.10 summarizes some weakness points of an Internet infrastructure.

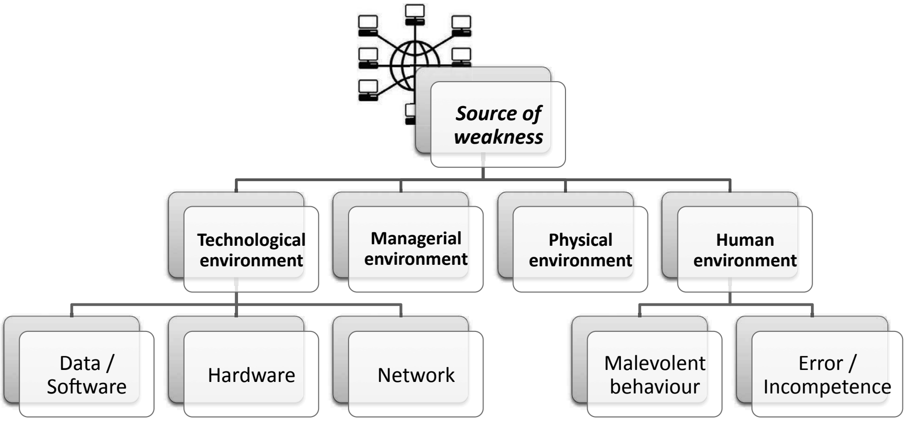


Figure 2.10 Some weak points in Internet infrastructure.

The Internet is vulnerable to cyber attacks

Most of the communication protocols used across the Internet can be misused to serve cyberattack purposes, and thus any systems connected through the Internet can potentially be the target of attacks. Figure 2.11 identifies some problems due to the misuse of technology or the lack of sufficient security measures.

Despite the evolution of computing technology in recent years, the basic Internet technologies (communication protocols TCP/IP, IP address) remain those implemented in its early days. New services have appeared without any change to the initial infrastructure, which was not designed to handle the flow of information to which we have become accustomed.

Security and data protection solutions were not initially integrated into Internet technologies. That they are now desirable is a result of the current use of the Internet having deviated so far from the original concept. Nowadays, it is a platform and enabler for commercial and financial transactions and critical applications for individuals, organizations, or states; this was not foreseen in its early days. What's more, every technology is fallible, and the complexity

[28] Chapters 3, 4 and 5 present some real cases of misappropriation of Internet for criminal purposes.

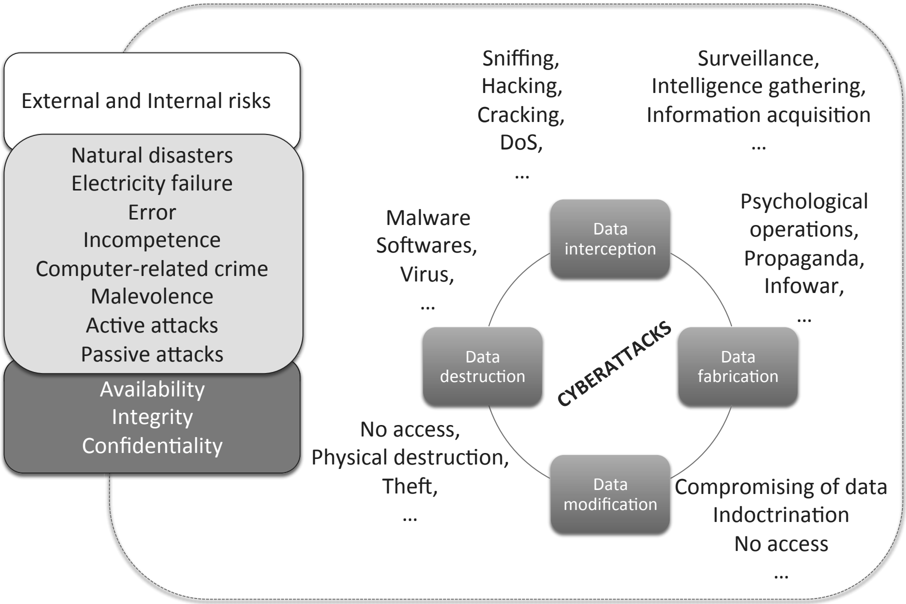


Figure 2.11 Security breaches and impacts.

of the technological environment is so vast that vulnerabilities will inevitably appear. The logic of the markets means that there is little encouragement for proposing robust technologies, and, moreover, there is no legal obligation for technology providers to market products with guaranteed levels of quality and security. All of these factors contribute to the current proliferation of security defects.

Security solutions do exist, but they can essentially be considered as *sticking plasters* applied to different places of the Internet's infrastructure to "block" (repair) each security breach. It is a technological approach that has the advantage of being adaptable to individual issues, but it addresses neither the problem of protecting the infrastructure nor that of protecting the assets associated with the Internet.

Cybercriminals take advantage of the characteristics of the Internet

The uncoupling of transactions from physical media (virtualization), communication tools involving encryption, steganography, and anonymity: these are factors that criminals in different countries can and do exploit. These factors enable criminals to collaborate at a distance, dispensing with physical meetings and operating in a flexible, secure manner – and with impunity. They can form teams, plan crimes, and carry them out, either in the traditional manner or by using information technologies. The global reach of the Internet allows criminals to act globally, on a large scale and rapidly.

The powerful possibilities created by the digital world and its underlying telecommunications compound the inherent problems associated with the design, implementation, management, and control of information technologies. Those inherent problems include crashes, malfunctions, technical and human errors, and natural disasters. On top of that, there are the vulnerabilities created by the interdependence of infrastructures.

The various forms of computer attacks in existence have in common a relatively low level of risk taken by the criminal, set against a potential for harm and damage that greatly exceeds the resources necessary to launch the attack. A number of factors enable criminals to carry out illegal acts without exposing themselves to significant risk (Figure 2.12). These include the ease of:

- carrying out digital identity theft, working anonymously via the identities of others, false identities, or by multiple intermediaries;
- working remotely via a number of proxies or intermediate systems, from different countries or from a digital paradise; and
- taking control of remote computers. The widespread availability of "hacks" that exploit system vulnerabilities, along with the libraries of attacks and software that build on criminal know-how all serve to exacerbate the situation. These factors, combined with the possibilities of remote action and of renting cybercrime tools and competences, encourage people to be criminals.

The Internet does not have any geographic borders because it is made up of different interconnected networks. Its geographical coverage is cross-border. The criminal benefits through this lack of territoriality of the Internet, through the inexistence in certain states of laws punishing ICT crimes, and through the multiple jurisdictions in which networks operate. In the same way as fiscal paradises, there exist digital paradises where a criminal can act or host both servers and illicit content with impunity. A person (or a piece of software) located in one country can initiate cybercrime activities that target and affect ICT resources in another, while utilizing resources and infrastructure physically located in a third country.

Prosecuting a crime, computer-related or otherwise, depends on national justice and police systems. Investigations into a cybercrime where traces, effects and participants are localized in different countries require extremely

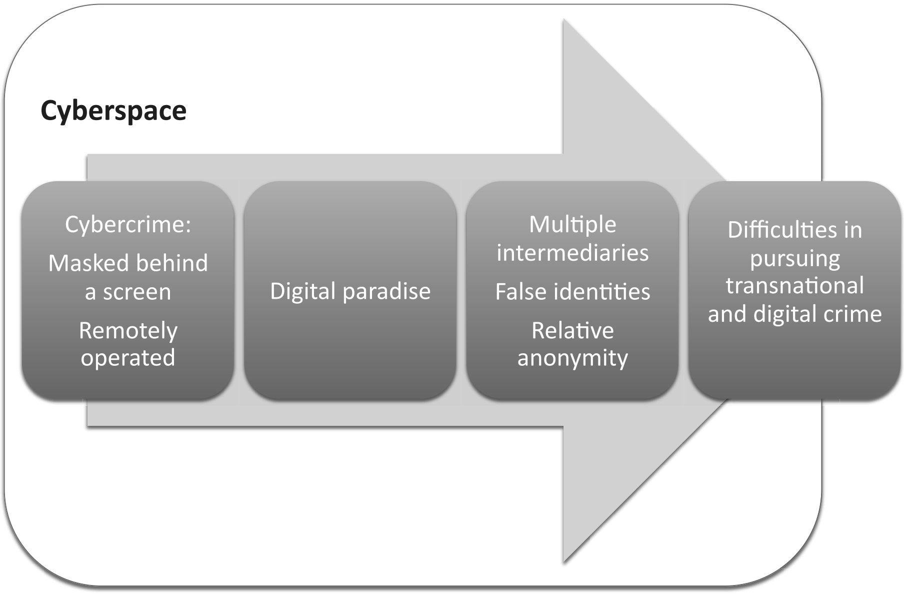


Figure 2.12 The Internet as a protective environment for criminals.

effective international cooperation. Such cooperation frequently causes numerous legislative, juridical, strategic, and operational problems, as well as running into issues of organization, reactivity, and the efficiency of the justice process. The criminals know how to benefit from the difficulty of prosecuting cross-border computer crimes. They act in a cross-border way, through numerous intermediaries that block their identification and minimise fixed locations. Using more and more anonymization techniques, fake or stolen IDs, criminals decrease their risk of being identified and arrested. They can thus have a real sense of impunity as they develop their illegal activities. The different forms of computer crime, organized or not, present relatively small risks to their perpetrator. Moreover, the damage caused and the profits gained usually far exceed the resources necessary for committing cybercrimes and the level of risks taken to perpetrate them.

Furthermore, those who create *malware*, and those who diffuse, sell, or use them, are extremely well organized. Indeed, they are often very specialized. Furthermore, the splitting of tasks and risks and criminal responsibility is often so efficient that it becomes hard, even impossible, to identify and localize a criminal, even when an illegal act is observed. The organization of the work is sufficiently optimized in relation to specific tasks (*malware* creation, the localization or selling of *botnets*, impersonation or creation of fake identities, stealing of credit card numbers, creation of fake credit cards, spamming, etc.) that every criminal can work efficiently while also being extremely dynamic, mobile and flexible, in order to adapt quickly to targets and escape from counterattacks and police investigation.

A world of opportunities and optimal conditions for committing crime

Each technology has criminal potential and offers opportunities for manipulations that allow the carrying out of illicit activities. This is an intrinsic risk. The Internet does not escape from this rule, and the opportunist criminal world has learned to exploit the world of ICT for profit.

From the press

> New virus raids your bank account – but you won't notice. The best way to protect yourself from an online financial scam is to diligently check your bank accounts. At least, until now. […] an elaborate new computer virus that not only helps fraudsters steal money from bank accounts – it also covers its tracks. […] A new version of the widely prevalent SpyEye Trojan horse swaps out banking Web pages preventing account holders from noticing that their money is gone.[29]

Cyberspace, due to its characteristics, offers a favourable environment for the expression of criminality, be it classical or related to exploiting the possibilities generated by information technologies. Additionally, it allows users to operate remotely, via networks and hidden behind a screen. In fact, some individuals may stray across the boundary into criminal action without ever being fully aware of the criminal nature of their acts.

The computer world offers cybercriminals the possibility of automating their activities. The rise in criminal actions, undertaken at distance through networks, against numerous targets and on a large scale, means that criminals can be ubiquitous in time and space. The dematerialization of transactions, communication facilities, and encoding and anonymity solutions provides connections between criminals without any physical contact, in a secure and

[29] Source: http://redtape.msnbc.msn.com/_news/2012/01/06/9986119-new-virus-raids-your-bank-account-but-you-wont-notice

flexible way. Therefore, they can organize themselves into teams and plan illicit actions to be performed either in a traditional way or through ICT.

The principal characteristics of computing technologies and of the Internet that are exploited for criminal ends are listed here.

- The digitalisation of information: digital information is fragile. It can be infinitely copied without being able to distinguish the copies from the originals. Moreover, stealing information is copying it: the information is not destroyed; it still exists, as opposed to a stolen wallet, whose owner knows that it is gone because it is no longer in his possession. So information theft and espionage are very difficult to precisely evaluate.
- The attack or cybercrime has the capacity to pass unnoticed by its victims.
- The virtual aspect of the people involved: there is no physical contact between people (victims and attackers). So it is easer to harm people and to impersonate them without facing them.
- The technologies (tools, services, hardware, software) have vulnerabilities exploited by the wrongdoers. The technologies are so complex that there are always vulnerabilities. In addition, securing an ICT environment connected to the Internet is a difficult and complex task.
- The network allows the putting into contact of people, systems and data: resources through the Internet are open to everyone and are accessible from all around the world. They constitute attractive targets, exposed to the criminal world that considers them as items of value and a source of direct (or indirect) enrichment. The Internet can be seen as a favourable context of opportunities for criminals.
- The ever-increasing number of users: as the number of people and systems increases, the potential targets for cyberattacks rises, and the more cybercrime is fruitful. The number of users and interconnected systems creates a huge market for crime.
- The existence of digital paradises: some countries have no laws relative to computing crime. In some countries, some malicious cyberactions are not considered criminal. The criminals can therefore attack distant systems and commit computing offences without fear of the consequences. The feeling of impunity is a driving force for criminals.
- The difficulties, and sometime impossibility, of correctly identifying the origins and perpetrators of an attack decrease the risks for the criminal to be identified, localised and taken. Moreover, digital traces can be

> hard to gather, store, and use as evidence in a court of law. Additionally, difficulties in prosecuting computing cross-border crime exist, and sometimes international cooperation is not sufficient.

Furthermore, information is at the heart of the strategies of criminal organizations. ICT therefore factors in the performance of criminality. Criminals organize themselves around the exchange of information, thanks to ICT. The networking of people and competencies permits the creation and operation of highly efficient, dematerialized criminal organizations.

The specialization, the high degree of financial competencies, and the professionalism required to commit financial crimes mean that these are particularly apt to being facilitated by ICT. The Internet contributes to the acquisition of information, better knowledge of the environment, and thus to criminal opportunities. Financial cybercrime requires technical competencies and know-how of the digital world. Because of the Internet, financial crime is not exclusively the domain of organized criminality. ICT brings it within the reach of isolated individuals. They can group together to a greater or lesser extent, but this is not always necessary. Cybercriminals can essentially be criminals with a feel for ICT or computer specialists with a feel for criminality (Figure 2.13).

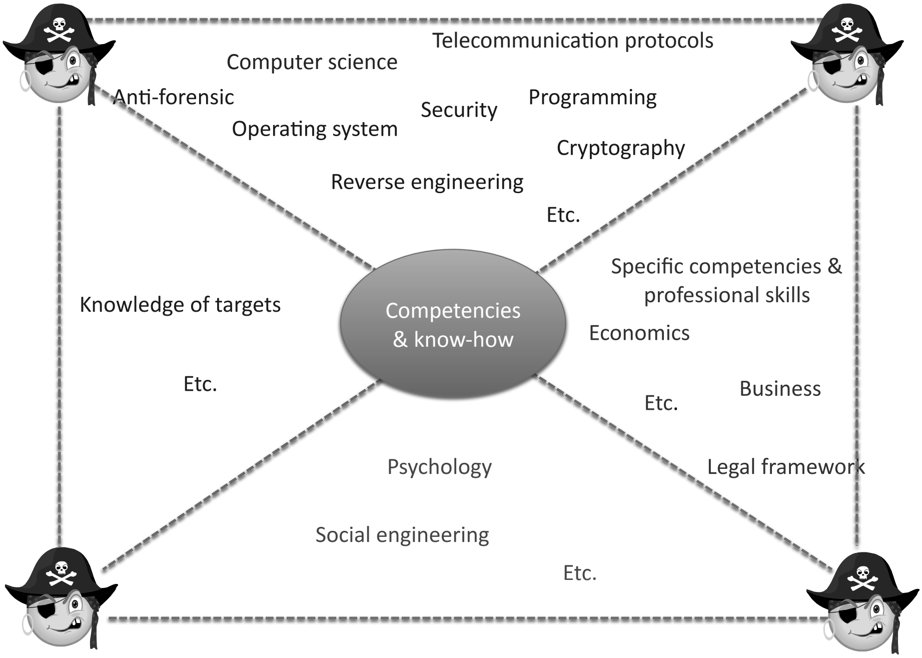


Figure 2.13 The competencies of cybercriminals.

Using the Internet, criminals can perpetrate illegal actions, with relative impunity, in exceptionally favourable conditions. Their risk-taking is minimal in relation to the profitability provided by a global sphere of action. So, cybercrime has contributed to the development of a context of insecurity, which is most often invisible, although sizeable threats are capable of hitting anywhere at any time. Cyberattacks have now become a genuinely harmful and destabilizing instrument for organizations and states.

A new paradox

There does exist a real paradox to the extent that most actors in the Internet chain can take advantage, in different degrees, of malevolent tendencies at the same time as they are falling victim to this criminality. Cybercrime can generate costs and be a source of benefits for some legal enterprises.

Through the diffusion of *malware*, the unauthorized access to computers, attacks targeted at damaging competitors, or business spying, cybercrime generates costs related to protection, reaction, and repression. An economy has developed around:

- security and legal advice;
- audit and evaluation of ICT security policies and measures;
- development and selling of security solutions and computing investigation tools;
- ICT security, legal and criminal science awareness, education and training;
- public and private research in previously quoted activities, but also in human and social sciences or computing.

The ICT security market responds to the underground cybercrime economy that enriches specific entities by harming society overall. Indeed, the costs generated by cybercrime, be they directly linked to justice and the expenses of policing, or incurred indirectly through the malfunction of businesses, are in the end borne by society.

Nowadays, viruses are professionally designed and are vectors of economic criminality that generate profit. They are extremely sophisticated, less and less visible, more and more profitable, and hardly detectable. *Botnets* are networks formed of “zombie” machines, infected by malevolent software and remotely controlled by a pirate. They contribute to the diffusion of *spam*, while the *botnets* grow through spamming, by infecting other computers.

Spamming is the massive diffusion of e-mails, and represents, according to different sources, such as the *Spamhaus Project* or the *Messaging anti-abuse working group*,[30] 85 to 90% of all transmitted e-mails. The production and diffusion of malevolent programs (*malware*: viruses, Trojans, *backdoors*, keyboard sniffers, *botnets*, etc.) and pirating tools has allowed the development of a real underground economy around a very profitable market. This has contributed simultaneously to growing the list of assets linked to information technologies for legal enterprises. Here are two examples. The virus market encourages the antivirus one. It adds to the enrichment of antivirus providers and sellers, and also to security advisers who are acting both legally and ethically. Spamming, on the other side, contributes to enriching:

- the providers of anti-spamming solutions;
- businesses that use spamming as a marketing and advertising tool, that some consider aggressive, but without being illegal;
- illegal entities that take control, through spamming, of the user's machine, install *malware*, steal personal data, and impersonate that user in order to commit other crimes.

2.4 Summary in 10 tips

1. The universal adoption of Internet technologies, the reliance of organizations and states on these technologies, and the interdependence of these infrastructures have introduced a significant degree of vulnerability into the everyday operations of these institutions.
2. Many vulnerabilities and threats exist that endanger any activities performed over the Internet. From natural disasters to malicious acts, passing through errors or absences of internal control and management, a wide range of incidents can occur bearing a negative impact on Internet activities.
3. Cybercrimes can take the form of traditional kinds of crime, such as money-laundering, blackmail, and extortion, although committed using new technologies. At the same time they can take the form of new types of crime, such as system intrusions, the theft of processor time, and the theft of source code or databases, all based on digital technologies.
4. Problems in the design, implementation, management, and control of computing environments, as well as problems arising from breakdowns,

[30] Respectively http://www.spamhaus.org/ and http://www.maawg.org/

malfunctions, mistakes, incompetence, or natural disasters, means that by their very nature, digital infrastructures display a certain level of insecurity. There are numerous possibilities for exploiting these failures for malicious ends.

5. Tools to exploit vulnerabilities and pieces of software that consolidate criminal and technical know-how into single packages exist and are widely available. They facilitate the performance of computer attacks by offering them to a large number of potential users – and essentially to anyone who is prepared to pay. The availability of such tools makes it easier to commit criminal activity. Nowadays, computer experts with criminal tendencies and criminals with computer skills are both able to commit cybercrimes.
6. The cybercriminal does not take any physical risk. He is comfortably installed in his usual environment and acts at a distance, in contrast to a traditional thief, who has to manage the stress of being physically present at the scene of the crime.
7. Criminals exploit the managerial and technical vulnerabilities of the Internet. They take advantage of the absence of a harmonized international legal framework and the lack of effective coordination between law enforcement agencies. The Internet environment is exceptionally conducive to white-collar crime. From a criminal's point of view, there is minimal risk, a wide coverage of the crime (a lot of targets can be reached), and potentially lucrative profits.
8. When confronted with the synergies and the convergence of organised crime, financial crime, and cybercrime, a wide-ranging and complete response is required that will meet the needs of national security, personal security, and the security of assets both tangible and intangible. Cybercrime has become a plague on society that touches everybody and which must be fought by effective measures of prevention and reaction.
9. The changes and the insecurity created by the extensive uses of information technologies, be these criminal or otherwise, can no longer be ignored. The reality of this insecurity needs to be taken into consideration during the design, implementation, management, and use of security tools.
10. It is important to make all Internet users aware of the stakes involved in the management of security and criminality and of the elementary measures that, if they are clearly defined and explained and intelligently implemented, will reinforce the confidence of users in the digital world and reduce the number of criminal opportunities.

2.5 Exercises

1. What is cybercriminality?
2. What are the main characteristics of a cybercrime?
3. What are the characteristics of the Internet that can be exploited for criminal purposes?
4. What kinds of crimes and offences does the Internet facilitate?
5. Identify factors that explain the existence of cybercriminality.
6. How can cybercriminal proximity can be explained?
7. What could be potential targets of cyberthreats?
8. Why does the interdependence of infrastructures cause a security problem?
9. Why it is necessary to master cyber-vulnerabilities?
10. Why it is difficult to have a unique/universal definition of cybercrime?
11. What is the main difference between a deviant behaviour and a criminal one?
12. In what circumstances can ICT misuses be illegal?

Chapter 3

Cybercrimes Against Persons

3.1 Understanding the context

In general, cybercrimes against persons can be divided into the categories of defamation, dissemination of offensive material, harassment, incitement to commit crimes, swindling, fraud and abuse of all kinds (Figure 3.1).

3.2 Affecting people's dignity and integrity

Among the most common, even if not systematically recognised problems, are those behaviours that damage private lives, personal dignity, and integrity, such as pedophilia, human trafficking, slavery, online intimidation, harassment, or excessive surveillance. The use of dematerialized communication services potentially exposes Internet users to all kind of fake friendships or illusions and also to the possibility of accessing violent, indecent, or offensive pictures. To be convinced of this, one need only type the keywords "ex girlfriend" into a search engine.

False feelings of security and the reality of predators

People have massively adopted instant message services. They can now be confronted by many kinds of harassment, rumours, intimidation or virtual (and

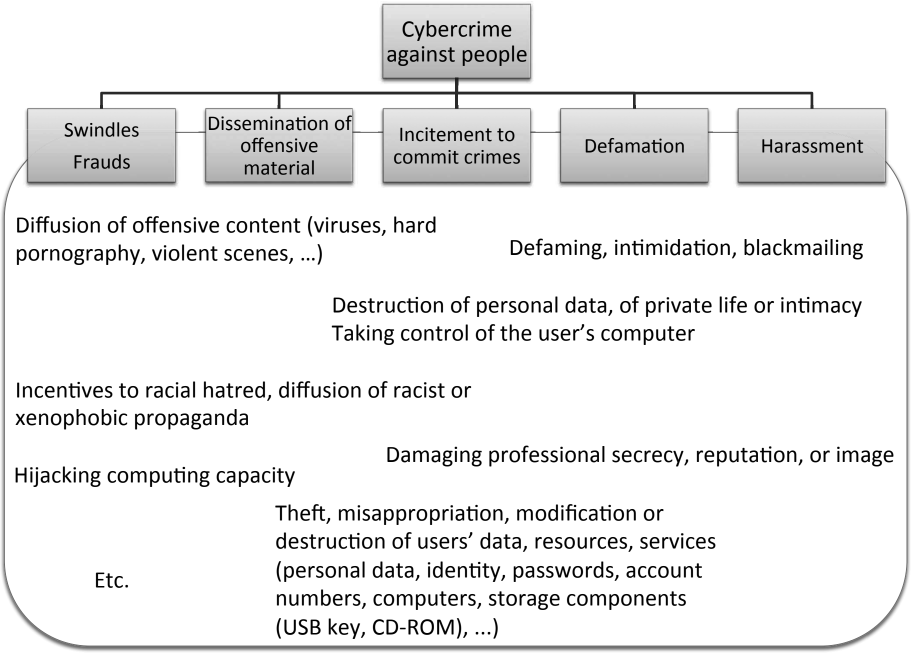

Cybercrime against people
Swindles
Frauds
Dissemination of offensive material
Incitement to commit crimes
Defamation
Harassment
Diffusion of offensive content (viruses, hard pornography, violent scenes, …)
Defaming, intimidation, blackmailing
Destruction of personal data, of private life or intimacy
Taking control of the user's computer
Incentives to racial hatred, diffusion of racist or xenophobic propaganda
Damaging professional secrecy, reputation, or image
Hijacking computing capacity
Theft, misappropriation, modification or destruction of users' data, resources, services (personal data, identity, passwords, account numbers, computers, storage components (USB key, CD-ROM), …)
Etc.

Figure 3.1 The main Internet-enabled actions that can harm individuals.

sometimes physical) meetings, contacts that are not necessarily enjoyable. A need to be listened to, a desire to explore, and a feeling of naïve confidence can be exploited to incite Internet users (often, but not exclusively, children or teenagers) to reveal themselves. The use of fake identities or fake profiles contributes hugely to deceiving or manipulating them. This is not restricted to the use of instant messenger services, but also, for example, to personal blogs, which are for some users genuine online intimate diaries or social networks.

The access providers themselves support this feeling of confidence. To cite only two examples of slogans that have figured in the past:

- MSN Web Messenger – "MSN Web Messenger allows you to discuss online with parents or friends simply by using a Web navigator! Use it on a public computer, at school, at work or at a friend's house: Everywhere where you can't install MSN Messenger"[1];
- Facebook – "Facebook is a social utility that connects you with the people around you."[2]

[1] webmessenger.msn.com

[2] http://www.facebook.com/

Nowadays people can use not only the Internet but also cell phones to harass, intimidate or threaten others, behaviour in which they might not indulge face-to-face. The relative anonymity and fake profiles that communications services offer also contribute to the proliferation of such behaviour.

From the Internet Crime Complaint Centre (IC3)

> *The Dangerous Side of Online Romance Scams*
> […] scammers target individuals who search for companionship or romance online. […] the online contact could be a criminal sitting in a cyber café with a well-rehearsed script that scammers have used repeatedly and successfully. Scammers search chat rooms, dating sites, and social networking sites looking for victims. The principal group of victims is over 40 years old and divorced, widowed, elderly, or disabled, but all demographics are at risk. Scammers use poetry, flowers, and other gifts to reel in victims, the entire time declaring their "undying love." These criminals also use stories of severe life circumstances, tragedies, deaths in the family, injuries to themselves, or other hardships to keep their victims concerned and involved in their schemes. Scammers also ask victims to send money to help overcome a financial situation they claim to be experiencing. These are all lies intended to take money from unsuspecting victims […] Victims who have agreed to meet in person with an online love interest have been reported missing, or injured, or in one instance, deceased.[3]

Fake profiles are common, and predators of all kinds have demonstrated great ability in acting as a confidante or a friend. Phases of seduction, for want of a better word, persuade youngsters to provide personal information, pictures, or even videos, often of an increasingly suggestive nature, and to go as far as to set up meetings. What is pernicious in this procedure is the gradual spiral into which the person is sucked, often based on feelings of shame or guilt that can be enhanced by threats or rewards. Usually things begin with very normal exchanges, banal questions and answers between friends that do not provoke any distrust, and these questions become progressively more and more intrusive, precise and personal.

Nothing keeps either minors or pedophiles from being present on a social website, for example. The latter can use this communication tool, and a favourable environment, to establish electronic relationships that could lead to sexual acts in front of a webcam (cybersex) or to real meetings – all of this without constraint. The true danger perhaps comes from the fact that social

[3] http://www.ic3.gov/media/2011/110429.aspx

networks are used in an environment of trust that cannot be ensured in any reliable or enduring way. The impression of being “between friends” creates a false feeling of confidence that can have a negative effect on people’s lives, especially children. Needless to say, juvenile pornography, the exploitation of children online, the seduction of a child through the Internet, or the possession of movies, pictures or documents that show the aggression or sexual exploitation of a child are all thoroughly illegal.

More than pornography

The Internet makes it possible for virtual communities to form around practices that are subject to legal sanction. This may involve pornography, pedophilia, or so-called snuff movies (a pornographic film that is supposed to show the actual murder of one of the performers at the end of a sadistic act). This type of crime is commonly linked to human trafficking, which most often involves women and children. Films and photos can be shared with little risk of police detection. As the relevant servers are frequently located in countries where law enforcement is absent or ineffectual, and with the use of private Internet relay chat (IRC) services for very limited periods of time, peer-to-peer (P2P) exchanges greatly increase the unencumbered action of criminals.

Several national laws ban sexual abuse and child sex abuse.[4] Here we consider some examples.

- The Swiss penal code (197 CPS), outlaws any person who manufactures, imports, stores, puts in circulation, promotes, exposes, offers, shows or makes available objects containing sexual acts with children, animals, excrement, or including/understanding acts of violence.
- The United States of America, to take another example, (18 U.S.C. &sect. 2251 and 2252) outlaws the possession, creation, sale, marketing, advertising, transmission, reception, trafficking, or any other dealing in child pornography.
- The Government of India clearly considers online pornography a punishable offence (The Indian Information Technology Act 2000, Chapter XI Para 67). Moreover, the Indian Penal Code, 1860 section 293, also

[4] *Terminology from Interpol:* “A sexual image of a child is *‘abuse’* or *‘exploitation’* and should never be described as ‘pornography’. Pornography is a term used for adults engaging in consensual sexual acts distributed (mostly) legally to the general public for their sexual pleasure. Child abuse images are not. They involve children who cannot and would not consent and who are victims of a crime. The child abuse images are documented evidence of a crime in progress – a child being sexually abused”. http://www.interpol.org/Public/Children/SexualAbuse/NationalLaws/Default.asp

specifies, in clear terms, the law against the sale, etc. of obscene objects to minors.

From Interpol

> Crimes against children are facilitated by the Internet, the increased use of which in recent years has led to a huge rise in offending. Not only can offenders distribute and access child abuse material more easily, but they can also come into direct contact with children – via chatrooms and social networking sites.[5]

Child abusing criminals can profit by the non-existence of laws or the variation of legal age for sexual activities to store child pornography on servers in countries that do not have relevant laws or in states where the age of sexual activities is considered irrelevant to crime.[6] The Internet is a means for cybercriminals to produce and distribute pornography related to child abuses. Pedophiles may use the Internet to contact children in order to subject them to sexual abuse. Crimes specifically against minors include the dissemination of pornographic messages that may be seen by minors. Cyberpedophile crimes are mainly investigated and prosecuted in developing countries.

From the Press

> United States officials said they uncovered an international child pornography network and arrested 72 people who used an online bulletin board called Dreamboard to trade tens of thousands of images and videos of sexually abused children […][7]

The Internet can also facilitate the industrialized and large-scale practice of human trafficking. Most often, victims of human traffic come from less developed countries. Among crimes against persons, other examples include infractions regarding privacy, personal image, professional confidentiality, and data privacy rights.

[5] http://www.interpol.org/Public/Children/SexualAbuse/NationalLaws/Default.asp

[6] This is demonstrated in particular by the statistics given by the Internet Watch Foundation during the past ten years – Internet Watch Foundation, IWF reveals 10 year statistics on child abuse images online (www.iwf.org.uk).

[7] Cebu Daily News: U.S. arrests include Philippine Felons, 5 August 2011
http://newsinfo.inquirer.net/36721/us-arrests-include-philippine-felons

Examples of the misuse of the Internet

There exist websites such as SeekingArrangement.com which describes itself as being "The premier dating website for Sugar daddies, mommies and babies." The qualifier "sugar" is clear when you see the website: "Mutually Beneficial Relationships." It is not strictly speaking a prostitution website, but more a place of mutual help where charitable and generous benefactors and benefactresses contribute to the personal development of other people. In same register, the websites seekingmillionnaire.com or seekingfantasy.com are unambiguous about the nature of their services. Whatever terminology is employed, the objective is to facilitate, through the Internet, transactions wherein the main components are money and sex.

Websites contributing to the sex industry and human trafficking are widespread and are often supplemented by auction websites or small ads where escort girl advertisements are common. Sex workers now offer their services on the Internet and on auctions. It is no longer a secret that websites such as Craigslist are used as means of facilitation and promotion of pornography, even pornography that includes or implies the participation of children or babies, and prostitution. Even young people looking for casual prostitution can use these sources. This was confirmed by a special report on Craigslist and child pornography by the U.S. Department of Justice's Child Exploitation and Obscenity Section (CEOS), National Center for Missing & Exploited Children (NCMEC).

All kinds of advertisements can find their public: for example, there have been advertisiements looking for a suicide partner, without beginning to count the live video broadcasts on the Internet of suicides. Intentional or not, the online overdose death in January 2003 of a 21 year old man was a classic case, as was as the webcast hanging of a 42-year old British man in 2007.[8] This is no longer a series of isolated events; many other cases are regularly reported by the media. The live broadcast of a death via webcam is a reality that particularly concerns adolescents.

What are the motivations and responsibilities of the exhibitionists and the viewers? As a general principle, who is the guiltiest: the service provider or the user? Is viewing such content an activity that can be compared to receiving stolen goods?

[8] http://en.wikipedia.org/wiki/Brandon_Vedas, and http://en.wikipedia.org/wiki/Kevin_Whitrick

Cyberstalking and cyberbullying

The Internet can also be used by cybercriminals to distribute harmful emails harassing, threatening or defaming people. Internet users can even now find online malicious sites that purport to provide contract murder planning.

Many incidents involve the distribution of women's personal information, often resulting in online harassment as in the case, for example, where a man posted a "sex-for-hire" advertisement on a country-based server that included the telephone number of his estranged wife; the woman received many obscene calls. In other cases, a man has logged on to Internet chat rooms using the identity of a woman and disclosed her telephone number, or a man has posted obscene, defamatory and annoying messages about a divorced woman in a Yahoo message group; these victims received many harassing phone calls.

The Internet is used to harass and intimidate people as a new modus operandi for the traditional offence of stalking. *Cyberstalking* is the use of information and communication technologies (internet, telephony, etc.) for the purposes of stalking, resulting in online harassment or abuse.

From the National Center for Victim of Crimes (USA)[9]

> *Potential Effects of Cyberstalking*
> Just because cyberstalking does not include physical contact with the perpetrator does not mean it is not as threatening or frightening as any other type of crime. Victims of cyberstalking often experience psychological trauma, as well as physical and emotional reactions as a result of their victimization. Some of these effects may include: changes in sleeping and eating patterns; nightmares; hypervigilance; anxiety; helplessness; fear for safety; shock and disbelief.[10]

Unwanted communications that may contain abuse or threatening or inappropriate words or images, directed by individuals at specific targeted persons to do persistent harassment, are considered as cyberstalking. Another form of cyber-harassment refers to the use of a perceived or real position of power or authority to attempt to annoy, frighten, or hurt a person, or to make somebody do something they are unwilling to do, through, for example, e-mail, instant messaging, text messages, websites, blogs, or mobile phones. An instance of

[9] The National Center for Victims of Crime is a nonprofit organization that advocates for victims' rights, trains professionals who work with victims, and serves as a trusted source of information on victims' issues. http://www.ncvc.org/ncvc/main.aspx?dbID=dash_Home

[10] http://www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer&DocumentID=32458

this could be the decision of an employee to impact a corporation by sending harmful emails in order to damage the firm's reputation. The content of the emails could be deliberately obscene, vulgar, abusive, intimidating, humiliating, and defamatory in nature.

From the press

How I became a Foursquare cyberstalker
It's the coolest social networking tool in the world. But is the geo-location app Foursquare a stalker's dream? Just how easy it is to uncover the intimate details of a complete stranger's life? Louise has straight, auburn hair and, judging by the only photograph I have of her, she's in her 30s. She works in recruitment. I also know which train station she uses regularly, what supermarket she shopped at last night and where she met her friends for a meal in her home town last week. At this moment, she is somewhere inside the pub in front of me meeting with colleagues after work. Louise is a complete stranger. Until 10 minutes ago when I discovered she was located within a mile of me, I didn't even know of her existence. But equipped only with a smartphone and an increasingly popular social networking application called Foursquare, I have located her to within just a few square metres, accessed her Twitter account and conducted multiple cross-referenced Google searches using the personal details I have already managed to accrue about her from her online presence. In the short time it has taken me to walk to this pub in central London, I probably know more about her than if I'd spent an hour talking to her face-to-face. She doesn't know it yet, but Louise is about to meet her new digital stalker […][11]

Threatening, observing a person's Internet activities, violations of privacy, and indeed every activity that causes fear or emotional distress by means of unsolicited e-mails, viruses, unwanted electronic communications, defamatory or derogatory statements, or negative rumours on webpages, forums, bulletin boards, chat rooms, etc, can be grouped together as cyberstalking, or as *cyberbullying* when young people are involved.

From stopcyberbullying.org

Cyberbullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has

[11] L. Hickman; The Guardian, 23 July 2010; http://www.guardian.co.uk/technology/2010/jul/23/foursquare

to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is NEVER called cyberbullying.[12]

Hate speech

Hate speech can take different forms, but in general targets individuals or groups on racial, ethnic, religious, gender or sexual grounds, or based on other characteristics such as physical or mental disabilities. Online hate speech often takes the form of websites and associated chat rooms and bulletin boards established by organized political groups (far right, ultra-nationalist, white supremacist, neo-Nazi, extreme Christian fundamentalists, anti-abortion, etc.). Most often these websites are designed to target young people and do not hesitate to use video games to incite or urge the elimination of Black, Jewish or Arab people, for example. Several thousand hate speech sites exist.

The Web provides the extremists with an efficient and cost-effective means of communication for reaching a potentially global audience. Acting remotely and in anonymity reduces the risk of identification and prevents the perpetrators from being prosecuted under national anti-hate speech laws.

The dissemination of racist and xenophobic material through computer systems, racial and xenophobically motivated threats, racial and xenophobically motivated insults, denialism, gross minimization, approval or justification of genocide or crimes against humanity, and aiding and abetting are criminalized in the Additional Protocol to the Convention on Cybercrime (ETS 189).

From the media

Hate speech infiltrates social-networking sites, report says – The unregulated nature of the Web has aided a proliferation of cyber-hate, according to a report the Simon Wiesenthal Center for Tolerance releaseda few days ago. The report, Digital Terrorism and Hate 2010, notes that there are about 11,500 hate-affiliated Web pages, a 20 percent jump from last year's study. According to the Wiesenthal Center, personal blogs as well as mainstream social-networking sites such as Facebook, MySpace, YouTube and Twitter are easily flooded with racist and terrorist-related content.[13]

[12] http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html

[13] CNN – Jesse Solomon, March 15 2010; http://articles.cnn.com/2010-03-15/tech/hate.speech.social.networks_1_web-sites-hate-social-networking-sites?_s=PM:TECH

3.3 Swindles and frauds over the Internet

Overview

Because using the Internet for the access or publication of information has no limits, and because cybercriminals are ingenious, the possibilities for committing cyberoffences are uncountable. However, even though it is impossible to describe in any exhaustive way every possible derivative, a simple outline of the principal risks for Internet users can still be proposed. It can be based on the different complaints received by governmental agencies fighting against cybercrimes.

The Swiss Confederation website MELANI publishes quarterly reports developed with the National Service for the Coordination of the Struggle Against Crime on the Internet (*Service national de coordination de la lutte contre la criminalité sur Internet, SCOCI*), on the subject of "Information Security: the situation at a Swiss and International level." A large amount of advice is also given to make people sensitive to the principal cyberabuses (child pornography, spamming, Nigerian letters, phishing, pyramidal system, frauds, etc.) to which they could fall victim.

In the U.S., for example, annual reports published by the Internet Crime Complaint Center (IC3) lead to an understanding of recognised types of fraud. These reports present a general indication of trends, categorizing and regrouping similar offences into generic families. The same type of swindle can have different variants and become more sophisticated as time passes.

The IC3, which is a result of a partnership between the FBI, the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA) received in 2011 a 3.4% higher number of complaints (314,246 to be precise) than in the previous year. The financial losses resulting from these incidents are estimated to be 485 million dollars in 2011, compared with $256 million in 2008 and $173 million in 2005.

The average cost of a fraud is estimated to be approximately $1544, although only 36.9% of complaints mentioned financial loss. This could lead us to suspect that victims do not always report a fraud if the loss can be borne, certainly in comparison to the effort involved in complaining. In the United States, in 2008 (the last year for which this analysis is available):

- 14.8% of the plaintiffs were victims of a fraud of less than 100 dollars;
- 36.5% of the plaintiffs were victims of a fraud of between 100 and 1,000 dollars;
- 33.7% of the plaintiffs were victims of a fraud of between 1,000 and 5,000 dollars;

- 7.7% of the plaintiffs were victims of a fraud of between 5,000 and 10,000 dollars;
- 7% of the plaintiffs were victims of a fraud of between 10,000 and one million dollars;
- 0.3% of the plaintiffs were victims of a fraud of over one million dollars.

The IC3 2011 report provides interesting statistics on the nature of cybercrimes reported in the USA.[14]

The major fraud types reported in 2011 were as follows:

- work-from-home-scams (17,352).
- FBI impersonation scams (14,350).
- loan intimidation scams (9,968).
- romance scams (5,663).
- auto-auction fraud (4,066).

The top five reported crime types in 2011 were as follows:

1. FBI-related scams (35,764);
2. identity theft (28,915);
3. advance free fraud (27,892);
4. non-auction / non-delivery of merchandise (22,404);
5. overpayment fraud (18,511);

Common themes can be identified, above all the use of contacts at a distance to convince victims that they are dealing with somebody different.

These figures can only give an overview of part of the reality of cybercrime. Not every cybercrime is reported, or even identified by its victims. Moreover, victims very often will not take the time to report a cybercrime involving a small amount of money. Many criminals take advantage of this and devise frauds accordingly.

Cyberscams of all kinds

Swindles of all kinds are performed through the Internet and take advantage of the dematerialization of the actors. The extortion of funds from businesses is also common; this is frequently carried out through blackmail and

[14] The 2011 IC3 reports – http://www.ic3.gov/media/annualreports.aspx

DDOS (Distributed Denial of Service) attacks that threaten to block the company's activities, or by threatening to publish confidential data. Among the very well organized frauds to which Internet users can fall victim, in particular one finds (Figure 3.2):

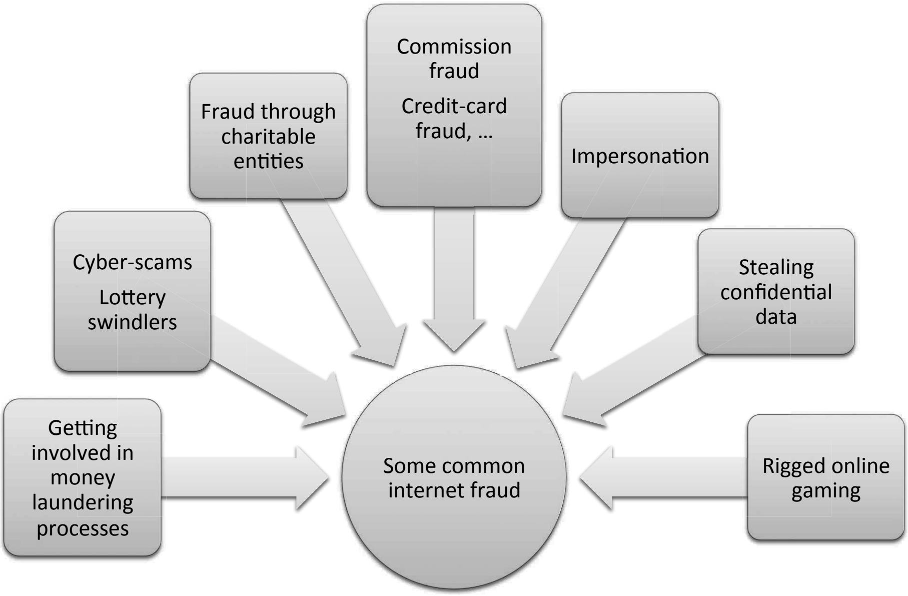

Commission fraud
Credit-card fraud, …
Fraud through charitable entities
Impersonation
Cyber-scams
Lottery swindlers
Stealing confidential data
Getting involved in money laundering processes
Some common internet fraud
Rigged online gaming

Figure 3.2 The most common Internet frauds.

- lottery swindles;
- rigged online gaming, forged bets with a possibility of compromising the participants;
- fraud through charity entities;
- computing fraud;
- commission fraud;
- money laundering;
- credit and debit card fraud;
- impersonation; and
- stealing confidential data.

These two last frauds are often performed by means of *phishing* actions, relying on the victim's credulity, naivety or helpfulness. By way of an example, the whole user community at the University of Lausanne receives from time to time the following e-mail:

> Dear unil.ch, holders of an account,
>
> this message is from the message center unil.ch to all the holders of an e-mail account. The Bureau of information technologies is in a migration process of all the e-mail addresses @unil.ch, in order to improve the services. If you don't want your account to be closed, you must give us as fast as possible the requested information for updating your profile and to be sure that your account stays active.
>
> "Confirm your EMAIL identity by sending back:
> Username
> Password
> Birth date
> Localization
> thank you for using unil.ch
> Warning code: VX2G99AAJ
> Kindest regards
> unil.ch Webmaster.

This was a *phishing* action, based on using a valid e-mail address and name from UNIL, in order to deceive the members of the University community and gather their identities and connection details. The end result of these attempts cannot be ascertained with any accuracy, but it can be assumed that the information they received could be used to generate spam, which would risk putting UNIL on a blacklist of sources of spam. The consequences of this could be that any legitimate e-mail sent from @unil.ch wouldn't be delivered, because it would be identified and rejected by some anti-spam filters. The consequences could also include the infection of the computing resources of the University, including employees' computers and servers dedicated to administration or scientific research, with the intention of propagating viruses, taking control of the computers to create zombie networks, stealing, modifying or destroying data from the UNIL servers, or performing distributed attacks.

Phishing schemes can be implemented through e-mails that direct victims to spoofed merchant websites that then mislead them into providing personal information, through SMSes (Smishing combination of SMS texting and phishing), or through telephony (Vishing).

From Interpol

> Sophisticated social engineering techniques are carried out on the Internet to trick people into revealing personal data, banking details and passwords. One of these

techniques is “phishing,” in which fraudsters create fake communications – such as emails, instant messages and pop up windows – that may appear to come from a legitimate source.[15]

From the FBI

You receive a text message or an automated phone call on your cell phone saying there’s a problem with your bank account. You’re given a phone number to call or a website to log into and asked to provide personal identifiable information – like a bank account number, PIN, or credit card number – to fix the problem.
[…] Online auction and classified ad fraud, where Internet criminals post products they don’t have but charge the consumer’s credit card anyway and pocket the money.
Delivery fraud, where online criminals posing as legitimate delivery services offer reduced or free shipping labels for a fee. When the customer tries to ship a package using a phony label, the legitimate delivery service flags it and requests payment from the customer. […] It could be a *“smishing”* or *“vishing”* scam […] and criminals on the other end of the phone or website could be attempting to collect your personal information in order to help themselves to your money. While most cyber scams target your computer, smishing and vishing scams target your mobile phone. […] Account holders at one particular credit union, after receiving a text about an account problem, called the phone number in the text, gave out their personal information, and had money withdrawn from their bank accounts within 10 minutes of their calls […]”[16]

Through prevention campaigns, many governmental agencies and police services regularly inform citizens about cyberfrauds, the precautions they should take, and the means of reporting problems.

In addition to personal data provided by users of their own free will, the means of losing personal data or having them stolen (outside cases of hacking) cannot be cannot be counted. Among the major methods are the loss or theft of a computer, a cell phone, or a USB stick. As an example, in October 2008 the German telecoms operator Telekom admitted to “having lost” the personal data of more than 17 million customers in the spring of 2006.[17]

[15] http://www.interpol.org/

[16] http://www.fbi.gov/news/stories/2010/november/cyber_112410/cyber_112410, 11/24/2010

[17] Wall street technology; M. Perez; 6 October 2008, “T-Mobile Lost 17 Million Subscribers’ Personal” http://www.wallstreetandtech.com/articles/210700232

From The FBI

> One of the most widespread types of cyber scam being perpetrated against consumers these days involves "scareware" – those pop-up messages you see on your computer saying you've got a virus, and all you have to do to get rid of it is buy the antivirus software being advertised. And if you don't buy it? The pop-ups continue unabated, and in some instances, the scareware renders all of the information on your computer inaccessible. […] Investigators discovered a variety of ruses used to infect computers with scareware, including consumers being directed to webpages featuring fake computer scans that instead downloaded malicious software. […] The FBI's Minneapolis office initiated an investigation into an international criminal group using online advertising to spread its scareware product, a tactic known as "malvertising."[18]

Nowadays festive periods are frequently exploited to spread malware. Commonly, greeting cards are used to infect carefully targeted information systems with malware. The receivers of these electroinc messages can thus find themselves exposed to links that claim to be to greeting cards but in reality, they forcibly install malware – and in spite of the presence of anti-virus software.

From LooksTooGoodToBeTrue.com

> "[…] An interesting point about fraud is that it is a crime in which you decide on whether to participate. Hanging up the phone or not responding to shady mailings or emails makes it difficult for the scammer to commit fraud. But con artists are very persuasive, using all types of excuses, explanations, and offers to lead you – and your money – away from common sense. […]"[19]

In another approach, fraudsters can set up entities that purport to be intermediaries designed to facilitate payments over the Internet. These entities are often linked to the use of auction websites. Of course, these intermediaries do not provide the advertised service of holding the purchaser's payment until the merchandise has been delivered in good shape, and then sending the money to the seller. These intermediaries keep the buyer's money without any delivery of the products that had been ordered.

[18] http://www.fbi.gov/news/stories/2011/june/cyber_062211/cyber_062211, 06/22/11

[19] http://www.lookstoogoodtobetrue.com/

The financial component of recorded frauds and the fact that the complaints relate to economic offences demonstrates that other types of frauds can affect Internet users independently of their age or technical abilities, even without needing to evoke the Internet problems of censorship, copyright infringement, press infractions, or website copying.

See the case study at the end of this chapter for more information on a FBI case related to an Internet fraud investigation.

From The Internet Crime Complaint Center (IC3)

Social network misspelling scam

During December 2010, the IC3 discovered misspellings of a social network site being used as a social engineering ploy. Misspelling the domain name of this site would redirect users to websites coded to look similar to the actual website. The website users were redirected to answer three or four simple survey questions. Upon answering those questions, users were offered a choice of three free gifts. Multiple brands were observed as being offered as gifts, including gift cards to retail stores and various brands of laptops. After clicking on one of the gifts, users were further redirected to other websites claiming to give free gifts for completing surveys. The surveys typically asked for name, address, phone number, and e-mail address. A user could spend hours filling out multiple surveys and never receive any of the gifts advertised.[20]

We should emphasise that it is not because the majority of cases cited in this book come from American sources that cyberfraud is restricted to the USA. Every country, every organisation, every Internet user can be a victim of cybercrime and the subject of a cyberfraud such as confidence tricks, advance-fee frauds, investment scams, and others.

Too good to be true

There are a number of frauds that exploit the credulity of Internet users by enticing them with the offer of winning free and easy money and require them to enter into the fraud voluntarily. Typically such frauds consist of asking the mark to start the transaction by communicating their personal and bank data and by advancing a sum of money to cover administrative costs. The victim

[20] http://www.ic3.gov/media/2011/110214.aspx

is persuaded to pay money upfront for further financial rewards that never materialize.

This particular kind of fraud began to be recognised two decades ago and was originally perfomed through the traditional mail system, typically with a Nigerian person requesting the help of an honest person to invest and launder money (Figure 3.3). The terminology "Nigerian Letters" is still used to describe this kind of activity, as is the name "419 Fraud" which stems from the relevant section of the Nigerian Criminal Code: Article 419; obtaining property by false pretences; cheating). Of course, this kind of advance-fee fraud is not restricted to Nigeria or Nigerians.

Variants of this phenomenon use "chains" or a "pyramid system." In order to qualify for a bigger commission, to avoid a catastrophe or bad luck, one has to forward a message to a certain number of contacts. The precise detail used to attract victims might be an inheritance, a lottery win, or human benevolence; the criminals do not lack in imagination for creating variants of well known frauds or for perfecting their approach by playing upon the financial, superstitious or sentimental aspects of their targets. Chains claiming to relate to magic or to solidarity, such as petitions, are usually fraudulent.

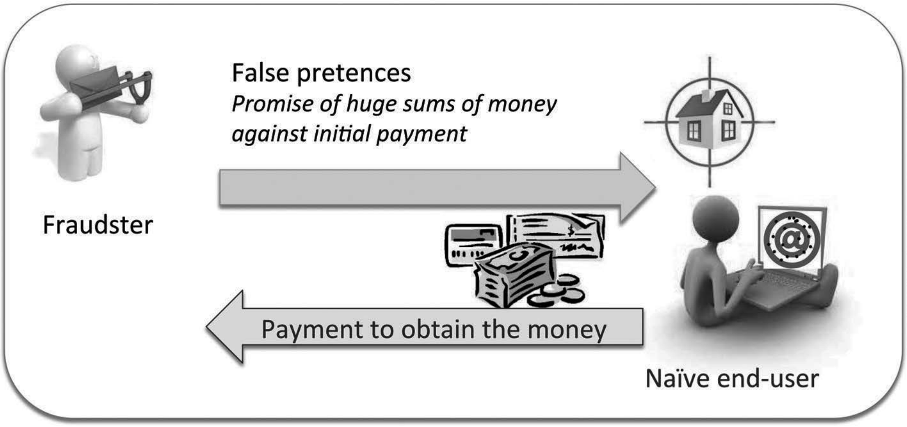

False pretences
Promise of huge sums of money against initial payment
Fraudster
Payment to obtain the money
Naïve end-user

Figure 3.3 Fake requests.

From Interpol

Lottery fraud is one of many different types of advance-fee fraud, where the perpetrator attempts to persuade a potential victim to pay fees in advance or relatively small sums of money for a service he or she has never asked for. In the case of a lottery scam, the money has to be paid for the transfer of a huge lottery win. Very often, names of popular companies or organizations are misused to give the lottery a trustworthy impression. Common media are the Internet, mobile devices and cell phones.[21]

From The Internet Crime Complaint Center (IC3)

Fraudulent FBI E-mail Being Sent by Lottery Scammers
The FBI has been alerted to a fraudulent email which purports to be from the FBI and attempts to convince recipients to send money to secure prizes won in an international lottery. The email contains Director Mueller's name and office address, and typically comes under the title, "FBI Internet Fraud Watch/Alert." The return email address may be listed as FBIfraudalert@hotmail.co.uk, or FBIfraudwatch@hotmail.co.uk. The email informs the recipient that the FBI, in conjunction with Scotland Yard, has been made aware that the recipient has won a substantial prize in a lottery, sponsored by a well-known corporation, in the United Kingdom. Recent variations of the phony lottery scams have claimed affiliation with Microsoft and MasterCard. The email goes on to explain that the FBI and Scotland Yard have screened the "Lottery House" and verified the transaction is legal. Both agencies have also examined the Lottery House's legal procedure and confirmed that it is legal as well. The recipients are directed to proceed with the transaction because their funds have been insured and the FBI and Scotland Yard are monitoring the transactions. This email and the associated lottery are fakes, as the victims are instructed to pay thousands of dollars in up-front fees to secure what eventually proves to be a non-existent prize. Consumers should be very cautious when notified they have won sweepstakes or lotteries they have not directly participated in. Consumers are further advised that situations requiring up-front payments to secure lottery or sweepstakes winnings are typically fraudulent.[22]

Most of the advertisements offering opportunities for working from home, using people to pass moneys through their bank accounts, remittances mainly received from abroad using services such as *Western Union* or *MoneyGram*, and instructing them to retain a sometimes substantial commission, are fraudulent. Electronic messages requiring financial agents as intermediaries or, more commonly, "mules," are massively and regularly sent out in order to recruit dupes who will subsequently be easily identifiable when judicial procedures begin. As a result of being involved, knowingly or not, in various frauds or money-laundering activities, these persons are considered as accomplices. Naivety or stupidity does not protect them from the legal consequences. The Internet user who responds to these kinds of invitations cannot verify whether

[21] http://www.interpol.org/

[22] http://www.ic3.gov/media/2006/060908.aspx

they would end up being involved in illegal activities and hence subject to legal consequences (Figure 3.4).

Cybercriminals are often behind advertisements for working from home, advertisements that might be published on websites, emails, on-line job finder services or social networks. The people who reply find themselves not only being used as mules for generalised money-laundering operations, but also find that their identities have been stolen.

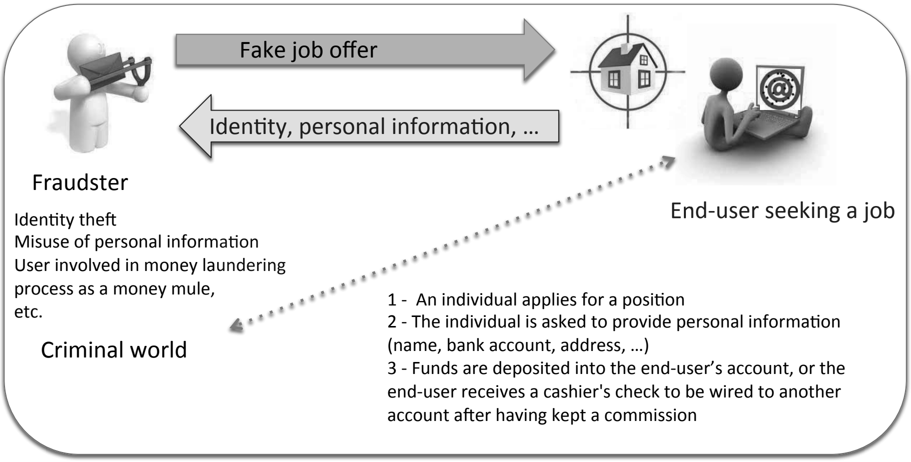

Fake job offer
Identity, personal information, ...
Fraudster
Identity theft
Misuse of personal information
User involved in money laundering process as a money mule, etc.
Criminal world
End-user seeking a job
1 - An individual applies for a position
2 - The individual is asked to provide personal information (name, bank account, address, ...)
3 - Funds are deposited into the end-user's account, or the end-user receives a cashier's check to be wired to another account after having kept a commission

Figure 3.4 A Work-From-Home Scheme.

The Internet washes whiter

Like all criminals who take advantage of the technological infrastructure, money launderers are increasingly using the Internet to convert money earned through criminal activities such as drug trafficking, the sale of illegal weapons, procurement, pedophilia, fiscal fraud, etc.

The Internet allows, with a great deal of impunity, the reinjection of dirty money into the economy through transactions, investments and the transfer of capital. Such transactions include market placements, the use of online casinos, e-commerce in selling (often fictitious) products for real money, thereby generating "justified" profits, e-banking, real estate through the Net, the creation of virtual entities or electronic wallets; these can all be used as conduits for money laundering. By their very nature these activities are difficult to control for the authorities, and undertaking appropriate legal responses is sometimes impossible. By participating in some of dematerialized activities, the individual Internet user can unconsciously assist in the development of money laundering. Businesses can also be implicated in these procedures and find themselves suffering the judicial and commercial consequences.

From The FBI

> *Foreign National Pleads Guilty to Role in International Money Laundering Scheme Involving More Than $1.4 Million in Losses to Victims*
> […] According to court documents, G. participated in a scheme that operated from July 2005 through November 2006, and involved the posting of fraudulent advertisements on eBay and other websites offering expensive vehicles and boats for sale that the conspirators did not possess. When the U.S. victims expressed interest in the merchandise, they were contacted directly by an e-mail from a purported seller. According to court documents, the victims were then instructed to wire transfer payments through "eBay Secure Traders" – an entity which has no actual affiliation to eBay but was used as a ruse to persuade the victims that they were sending money into a secure escrow account pending delivery and inspection of their purchases. Instead, the victims' funds were wired directly into bank accounts in Hungary, Slovakia, the Czech Republic and Poland that were controlled by co-conspirators.[23]

3.4 Identity crimes

Impersonation is the appropriation, without the agreement or consent of the interested parties, information that enables the identification of physical persons or organizations. This is commonly, if wrongly, known as *identity theft*. The difference between the two terms is that identity theft consists of taking the identity of a dead person (usually declared dead under another name) and impersonation is taking the identity of a living person. This can include the name, birth date, address, phone number, social security number, passport, ID, driver's license, student card, credit card, bank account or personal identification number (PIN), etc. Impersonation on the Internet allows, among other things, the purchase of goods and services for which the victims have to pay, the use of their rights or entitlements, or the performance of illegal actions under their name.

Impersonation can also be used when creating a fake profile on social networks, diverting email or falsifying a medical insurance number. Fraudsters hoping for free medical care carry out medical identity usurpation, making

[23] http://www.fbi.gov/news/pressrel/press-releases/foreign-national-pleads-guilty-to-role-in-international-money-laundering-scheme-involving-more-than-1.4-million-in-losses-to-victims Washington, D.C., 13 May 2010; Department of Justice (202) 514-2007.

false entries or supplying incorrect information or falsifying medical data in computerized medical files. Clearly this can have a negative impact on the healthcare that the victim receives. In such cases, the victims do not benefit from the same type of compensation as in the case of the manipulation of financial data. Furthermore, often the fact of having been the victim of this type of fraud is not recognised before the victim has indeed suffered the financial or health-related consequences.

The health sector is indeed very vulnerable to the theft or loss of data, as was underlined in the report on medical identity usurpation published in 2006 by the World Privacy Forum. In many contexts, especially in countries where medical insurance is not socialized, the only possibility for some people to have medical care is by medical impersonation. The *New York Times* ran a headline, on June 12, 2009, reading *"Medical Problems Could Include Identity Theft."* The article presented the case of a 37-year old man, the CEO of a big company in Texas, who had never had health problems, and who was surprised when he learned he owed several thousand dollars to healthcare providers.[24]

The manipulation of identities is an integral part of all criminal strategies and is not restricted to organized crime or terrorism. Impersonation on the Internet has taken on industrial dimensions and is now a real plague for the institutions or individuals that fall victim. "Confidential data of six million Chileans (addresses, personal phone numbers and tax declarations) have been published on the Internet over the last two days by a cyberpirate," reported Agence France-Presse on May 13, 2008. Nowadays, most crimes committed using fake identities or impersonations prevent, or at least delay, the identification and arrrest of the criminals.

From the FBI

> It began with a crooked "insider" who had access to a nearly unending supply of personal consumer information. It ended up *the largest case of identity theft* ever investigated and prosecuted in the U.S. – with 30,000 victims across the U.S. and Canada and millions of dollars in losses […] The "insider" was Philip Cummings, a help desk employee with a Long Island, NY, company that provided special software to its client companies – like banks and other financial institutions – allowing them to download consumer credit reports from the three major commercial credit reporting agencies. Cummings had access to his clients' codes and passwords, which meant he could download virtually all the consumer credit reports he wanted. And he did, after being approached by a ring of Nigerian nationals

[24] www.nytimes.com, 06.13.2009.

> who offered to pay for copies. Even after leaving the company, Cummings continued using his inside knowledge to download and sell credit reports to this identity theft ring for another two years […] Thousands of personal savings accounts were looted. Fake charges were racked up on credit cards. Addresses on bank accounts were changed so that new credit, check, and ATM cards were mailed directly to the thieves […] Federal authorities – the FBI, with the assistance of the U.S. Postal Inspection Service and the Secret Service – were called in to investigate when a major credit company discovered that thousands of credit reports had been downloaded without permission. Soon other companies were reporting the same thing. A review of the victim companies' 1800 phone records led investigators to the Long Island company that employed Philip Cummings […] and ultimately, to Cummings himself and his partners in crime. Last month, Cummings pled guilty.[25]

The phenomenon of identity theft over the Internet that began to take off in 2003 has continued to grow. It is thus a recurrent problem and not at all a recent one, as demonstrated by the case above that dates from 2004.

Digital identities

Changing one's identity in the real world is quite easy. The number of "real-fake IDs" in circulation testifies to this, as does the following case.

From the Press

> A mother of 24 quintuplets had her eyes bigger than her stomach. Murielle, who lives in Suresnes (Hauts-de-Seine, France), invented the existence of twenty-four sets of quintuplets by using a fake birth certificate. After it worked once, she created for herself twenty-four different identities, based on the details of genuine real mothers of quintuplets, which made 120 fictitious children. This thirty-four year old woman defrauded seventeen domestic insurance companies, earning 22,100 Euros a month (about 32,000 dollars). Two employees of one of the companies who worked in the same office were surprised to have two files relating to quintuplets to process and thus uncovered the fraud in 2006.[26]

On the Internet, having a fake identity to deceive people is extremely easy. It is easy to create an electronic identity that does not match reality, because the digitization of information grants to the Internet, in some sense, the power

[25] http://www.fbi.gov/news/stories/2004/october/uncoveridt_101504; 10/18/04.

[26] www.france.soir.fr, 09/35/2008.

of creating a virtual reality based on some parts of the truth. In a dematerialized world, where all information is merely a chain of binary numbers, how much can we rely on the virtual identity of a person or a resource? How can we be sure of the identity of the people with whom we interact, or the authenticity of messages, transactions, servers, or information?

A virtual identity has no direct link with the real identity of a person or resource. The proof is in the profusion of electronic addresses, aliases, and pseudonyms that can be used by a single person to communicate through e-mail, forums, instant messaging programmes, and other services. Depending on the context and the purpose of the communication, virtual names, digitalized avatars, pseudonyms, and aliases are in some way identical projections of the same identity. Identity has never been universal or recognized in the same way through time, culture, and society. But does having an alias on the Internet imply criminal action or intent? Can it not simply correspond to the desire to stay anonymous in order to communicate better, or differently, or not wanting to be responsible for illicit actions? Does it simply permit people to live in the shadows, hidden behind multiple identities and technological intermediaries? It allows us to live happily like the cricket in the fable of the 18th century poet, J.P. Claris de Florian, a protégé of Voltaire, who famously maintained: “In order to live happy, let us live hidden.”

We live in a society in which people teach their children to protect themselves from predators by never giving their real name or address on the Internet, that they should always create aliases. Thus protection on the Internet begins with an incitement to fake identities. It is an education, obviously with the intention of protecting the vulnerable, that is based on mistrust, deceit, and dissimulation. The identification and management of identities, including on the Internet, and the related risk of demarcation drift, will form one of the biggest problems of the years to come.

Finally, the globalization of computer crime, the need to protect the critical infrastructure of a country, personal data, and the Internet user’s private sphere, obliges us to rethink the notion of identity and its control on an international level. Above even a cyber-civic status that could be constituted and enforced by the root DNS[27] servers managed by the ICANN[28], there is the challenge of creating and maintaining a true Internet, one that is more trustworthy, safe, and identifiable. A considerable part of the modalities of modern society, such as identity, identification and authentication, rely on the common need to live together in a stable and safe world, virtual or not.

[27] DNS: Domain Name System.

[28] Internet Corporation for Assigned Names and Numbers (www.icann.org).

Examples of identity theft and fraud related cases from the United States Department of Justice

Central District of California. A woman pleaded guilty to federal charges of using a stolen Social Security number to obtain thousands of dollars in credit and then filing for bankruptcy in the name of her victim. More recently, a man was indicted, pleaded guilty to federal charges and was sentenced to 27 months' imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit $764,000 in counterfeit checks into a bank account he established.

Central District of California. Two of three defendants have pleaded guilty to identity theft, bank fraud, and related charges for their roles in a scheme to open bank accounts with both real and fake identification documents, deposit U.S. Treasury checks that were stolen from the mail, and withdraw funds from those accounts.

Middle District of Florida. A defendant has been indicted on bank fraud charges for obtaining names, addresses, and Social Security numbers from a Web site and using those data to apply for a series of car loans over the Internet.

Southern District of Florida. A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than $13,000 from the victim's bank account, and obtaining five department store credit cards in the victim's name and charging approximately $4,000 on those cards.

District of Kansas. A defendant pleaded guilty to conspiracy, odometer fraud, and mail fraud for operating an odometer "rollback" scheme on used cars. The defendant used false and assumed identities, including the identities of deceased persons, to obtain false identification documents and fraudulent car titles.[29]

Some thoughts on identification by biometric factors

On May 17, 2009, the Swiss population voted on the adoption of biometric passports to address, essentially, the need to protect identity documents and reinforce the verification of identity from a security perspective. The proposal passed by a slim margin (50.14%). This revealed both a genuine hesitation on the part of half of the population about the accepted solution and a hesitation about the effective guarantees over the security of personal data, both in the database and in the passport, and the non-surveillance or non-traceability of the citizen.

It should be admitted that these guarantees did not exist when the proposal was first made, and the justifications for the biometric passport were simply perceived as being unconvincing, vague, and muddled. Indeed, in spite of the

[29] http://www.justice.gov/criminal/fraud/websites/idtheft.html

question having been the subject of a referendum, the real debate in society only took place later, in rushed circumstances and with only limited participation by representatives of civil society. It must be hoped that this will be followed by a period of consideration led by citizens rather than technology sellers. Why should this subject provoke so many questions? Doubtless because the biometric passport is the point of convergence of four complex domains that emerge from different disciplinary fields: biometry, identity, IT technologies, and security.

Historically, since Alfonse Bertillon (a French criminologist who died in 1914) invented judicial anthropometry, biometry has been used to identify and record delinquents. Following from this, the adoption of the biometric passport has fed the polemic that recording such information is to consider all citizens like criminals. Biometry is a sensitive subject as it touches the very nature of living persons, their corporal intimacy and individuality. For each person, identity is a product of culture, history, origins, experiences, and affiliations, and is unique. The mutation of the concept of identity is progressive and can be traced through the evolution of societies and history. Each culture and each time possesses an individual model of identity. It would be unrealistic to think that an Occidental model, based on the patronymic name, could prevail everywhere around the world and be stable. The question of identity is old and complex, with multiple sociocultural aspects, and the answer to this question cannot be found through a particular technology, but rather through our relation to the technology, as a function of our history and civilization. It is a philosophical question that simultaneously touches human, social, political and legal sciences.

A major issue is that the electronic supports designed to solve identity verification problems still cannot answer the fundamental human question: "Who am I, Who is he?" The answer to this universal question cannot be unique or uniform, or, even less, coded onto a smart chip or in a database. The identity of a human being cannot be resolved to a chain of binary information, similar to a label on a product. The problem of biometric identity is in part linked to the globalization of the notion of identity. Is it desirable to globalize identity, when we would prefer to preserve a certain national and cultural identity? A deep approach to the problem of digital biometric identity is necessary, and this problem cannot be reduced to its technological or security components, nor be justified by fear, nor be tied to one single commercially-supplied solution.

With reference to the biometric passport and the centralized database with which it is associated, there are a number of different elements to take into account:

- nominative identity (a name that is a piece of information);
- a body part (that loses its corporality in order to become digital information);
- electronics (a smart chip);
- computing (computers, networks, databases).

What used to be relatively simple (an identity document containing basic information) becomes extremely complex because of the modification of the nature of its information, of the digitization, and of the transformation from a paper document to an electronic document that requires a robust computing infrastructure that, for the moment, we do not know how to control – or even if it can be appropriately protected.

The fingerprint is an image of a body part and conceptually remains something tangible and familiar to most people. But it is not the filing of the print, which is already widely performed, that matters, but its digitization. Where will it be stored, by whom, and how might it be manipulated? Once the process has begun, why should we limit ourselves to two prints and not ask for ten, and then the iris, the retina, etc.? Will we finish by digitalizing the DNA of individuals? Nothing should be excluded. Will we live a future where a microchip, a miniaturized biometric passport containing all of its information, will be injected under each citizen's skin, just as is currently done with identification chips for dogs?

If digitized data, such as digital fingerprints, come to be altered or modified in the database, by mistake or deliberately, the victim will face the challenge of proving their own identity in a context where their data differ from the binary encoded data on file. Humans might make mistakes, but computing resources can multiply them. For example, a major terrorism file in the U.S. has been criticised as containing 35% mistakes, according to a report of the American Ministry of Justice, published in May 2009[30]. The surveillance list of presumed terrorists that had been created by the FBI reported wrongly added hundreds of thousands of persons.

If the role of the biometric passport is to verify the identity of the holder, the existence of the central database is not justified. Indeed, during a check, the chip is used to authenticate the card as being a genuine document and possibly to compare the prints with their digital equivalents, without using a centralized database. The data contained in the passport are sufficient on their own to detect identity fraud. This type of solution has been implemented in Germany, for example. In addition, the nature and contents of the centralized

[30] http://www.justice.gov/oig/reports/FBI/a0925/final.pdf

database have subject to great criticism by data protection officials. In reality, a centralized database actually addresses different objectives and, by its nature, presents the following risks:

- cross-linking or aggregation of files relating to an individual;
- enlarging the contents of the database: it could contain all kinds of data, biometric or standard, DNA, behavioural data, data relative to health, politic opinions, religion, etc.;
- the future evolution of the use of the database by public authorities or commercial entities (which is already planned and involves other states and airline companies).

From the media

> *Loss of biometric data from 9 million Israelis* cause for concern – With governments and businesses collecting an ever greater amount of biometric data from individuals, the recent theft of an entire database containing biometric data on more than nine million Israelis is serious cause for concern […][31]

3.5 Privacy related offences

Privacy underpins human dignity and other values such as the freedom of association and the freedom of speech. It has become one of the most important human rights of the modern age. The *Oxford Advanced Learner's Dictionary* gives the following definition for privacy: "the state of being alone and not watched or disturbed by other people; the state of being free from the attention of the public." Nowadays, pervasive technologies that can observe, monitor or collect data, image, or sound can put privacy in danger.

About privacy and human rights in a digital world

Cyberspace is no Cyber-Wonderland. It is, instead, a potentially tough world. While everybody – young and old – joins the crowd on the web for entertainment or for business, the cyberscene, like the real world, is ruled by power and money.

To get free services, too many users deliver a huge amount of personal data and data on other people. Too many users do not understand the need for pro-

[31] http://www.homelandsecuritynewswire.com/srbiometrics20111025-loss-of-biometric-data-from-9-million-israelis-cause-for-concern; 25 October 2011.

tecting such data; they just ignore the issue. Personal data, user profiles, and consumer behaviours are modern goods that do have a market value. Business profitability kills privacy concerns.

All digital activities leave traces. Some people know how to hide or delete their traces on the web, while others collect, correlate, manipulate and use traces for their own goals. Data may even be collected legally, as protection laws are far from perfect or effective. Hidden activities of cyber-surveillance do exist, such as programmes spying on online-users. The major players on the Internet, and all kinds of e-commerce or service providers, accumulate customer data, claiming to use it in order to provide better service. The information is there, open to misuse, or to criminals who make a living out of cybercrime by stealing identities, rights and personal information.

Is privacy at all compatible with e-commerce that collects, delivers, and exploits personal data without the owners' explicit consent?

Data protection is a must to ensure self-determination, freedom of expression, human dignity, and democracy. Responsibly connecting the world includes emphasizing, for example:

- the 1980 OCDE Guidelines on Privacy;
- the 1995 Data Protection and the 2002 Electronic Communications Directives;
- the Madrid Privacy Declaration that reaffirms international instruments for privacy protection, identifies new challenges, and calls for concrete actions; and
- the 1998 European Convention on Human Rights (ECHR) and its Article No. 8: "Everyone has the right to respect for his private and family life, his home and his correspondence."

Human rights are never definitively acquired. They must not be infringed or bargained. We can no longer accept that personal data are being used like mere merchandise, as is actually the case in many countries.

International Privacy, in its 2004 report, specifies

> Privacy is recognized around the world in diverse regions and cultures. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights treaties. Nearly every country in the world includes a right of privacy in its constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently written constitutions include specific rights to access and control one's personal information. In many

of the countries where privacy is not explicitly recognized in the constitution, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the UN International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.[32]

About privacy and data protection

Privacy concerns not only the protection of information (information privacy) but also the protection of people's physical selves against invasive procedures (bodily privacy), protection of any form of communication (privacy of communications), and the protection of environment (territory privacy).

An example of a privacy offence is illustrated as follows: in 2000, a well-known singer's banking details were discovered on a second-hand computer discarded by a merchant banker. The PC was released into the second-user market without first being wiped clean of data.[33]

The importance of privacy issues in the information society has led several associations to fight against privacy threats and offences to help protect fundamentals rights. Among them, for example:

- Privacy International (PI)[34] is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, medical privacy, and freedom of information and expression.
- Electronic Privacy Information Center (EPIC)[35] is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberty issues, to protect privacy as detailed in the US constitution First Amendment,[36] as well as other constitutional values.
- Privacy.Org[37] is a site for daily news, information, and initiatives on privacy. This web page is a joint project of the Electronic Privacy Information Center (EPIC) and Privacy International.

[32] www.privacyinternational.org (PHR2004 – Overview of Privacy)

[33] http://www.theregister.co.uk/

[34] www.privacyinternational.org

[35] www.epic.org

[36] The First Amendment of the United States Constitution protects the right to freedom of religion and freedom of expression from government interference. Source: www.law.cornell.edu/wex/index.php/First_amendment

[37] www.privacy.org/

- CyberRights & CyberLiberties[38] (UK) is a non-profit civil liberties organization founded on January 10, 1997. Its main purpose is to promote free speech and privacy on the Internet and raise public awareness of these important issues. The Web pages have been online since July 1996.

Potential privacy risks are real because, very frequently, personal data are not protected. Data are transmitted and stored as plain text and can be used, for example, as commercial assets or be subject to cybercrime.

From Privacy.org

A pioneer of a country's DNA database said it may have grown so far beyond its original purpose that it now risks undermining civil rights. Hundreds of thousands of innocent people's DNA is now held on this database.[39]

From Interpol

Web of Victims: A Chilling Case of "Sextortion"

The hacker knew every move the unsuspecting victim made. He controlled her computer webcam and microphone. He could see her in her bedroom, hear her conversations, knew every keystroke she made online. And he threatened to expose her secrets unless she bowed to his demands. […] The hacker, who was arrested after a two-year investigation, used malicious code to infect and control the computers of his victims. Then he searched for explicit pictures from their computers, downloaded them, and used the images in an attempt to extort more pictures and videos from them.

After the hacker infected one computer, he used a popular social networking site – and a technique called "spear phishing" – to spread the virus. […]

In several instances, the hacker posed online as a young woman's friend or sister and sent messages with attachments asking if the victim wanted to see a scary video. Because the messages appeared to be from a trusted source, the victims usually didn't think twice about opening the attachment. When they did, the virus secretly installed itself, and the hacker had total control over their computers – including all files and folders, webcams, and microphones. Using similar spear phishing methods—posing as a friend or a trusted source – the hacker spread the virus through the social network like wildfire. Victims – particularly teenage girls – were understandably devastated when they learned their privacy had been so completely violated. Many were afraid to tell their parents about the situation. For example, the hacker attached a pornographic picture of one victim in an e-mail and

[38] www.cyber-rights.org/

[39] www.privacy.org/archives/001875.html

> demanded sexually explicit video of her in return for not telling her parents about the pictures he had downloaded from her computer. […] Unlike many computer intrusions, where a hacker uses malicious software to steal identities or financial information, this case was primarily about spying and extortion – or as our Los Angeles cyber squad more aptly termed it, "sextortion." [40]

A case related by the International Business Times

> *Facebook Login Risk: Ramnit Worm Steals User Details*
> A Ramnit worm has stolen the details of 45,000 Facebook user logins, according to a report. […] Seculert, a cyber threat management firm, has a research lab that identified a new variant of the Ramnit work, the company reports. The Ramnit worm was originally found in 2010 infecting Windows executable and HTML files and other sensitive information to steal. […] "In addition, cybercriminals are taking advantage of the fact that users tend to use the same password in various web-based services (Facebook, Gmail, Corporate SSL VPN, Outlook Web Access, etc.) to gain remote access to corporate networks," Seculert said.[41]

Some thoughts on electronic surveillance

The biometric passport represents, by its very nature, a relatively anodyne introduction into everyday life of computerized, automated, flexible, invisible and globalized surveillance. Indeed, remote reading, especially against the wishes of the individual carrying the information, introduces the problem of the traceability and automatic control of the population. The biometric passport's chip creates the possibility of being able to monitor citizens against their will. This implies a daily acceptance of such monitoring. Does the biometric passport introduce a risk of reducing an individual's liberties by using effective surveillance device? Should the chip reading only be permitted in a "contact" mode, meaning after insertion in a reader, so that the individual knows he is being checked?

In addition, the risks linked to the absence of control over the data (in the passport and in the database), by either the data owner or the person authorised to consult those data, provoke the following questions:

- Who will be authorised to access the data? How, and on the basis of which rights, will they access data?
- Who is watching the watcher? And how?

[40] http://www.fbi.gov/news/stories/2010/november/web-of-victims/web-of-victims, 11/02/2010

[41] IBTimes Staff Report; 6 January 2012; http://www.ibtimes.com/articles/277613/20120106/facebook-login-risk-ramnit-worm-steals-user.htm

- Who certifies, guarantees the availability, the reliability, and the security of the computing system?
- Who controls the security of the flow of information exchanged?
- What are the possible legal actions for a citizen in case of any problems?
- How can we effectively secure data when the security solutions that exist have already been broken?

The technologies used for the processing and communication of information do possess an intrinsic potential to be used against liberties. Besides, they form part of the strategies of the war against criminality and are key operational tools in the hands of the police.

Among the huge number of questions raised all around the world by the adoption of electronic and biometric identity files, let us focus on the following key ones:

- Does the biometric passport help the fight against clandestine immigration?
- Is the biometric passport an answer to pressures coming from a particular sector (solution, equipment, service, lectors, biometric solution, RFID, computing providers, industrials of microchips, etc.)?
- Can the biometric passport become indispensable in the provision of other services? Administrative purposes? Commercial purposes? Electronic signatures? Electronic transactions on the Internet? E-voting? Mean of payment? Daily life?

Just like other computing technologies, biometry is not neutral. They lead to profound modifications of our society that lead us to question our values. Biometry and computing technologies are powerful tools in the hands of those who control them.

3.6 Technological innovation and responsibility

A technological answer based on fear, industrialized or commercialized in order to satisfy some needs, while ignoring other aspects, in a logic of *business* benefiting private actors, cannot possibly constitute an appropriate response for civil society.

As far as technological innovations are concerned, it should be noted that most of the technicians or researchers whose job it is to produce technological or scientific progress, very often outside of political or social context, do not accompany their work with a reflection on the long-term consequences of the transformation of the society that their tools are likely to provoke. This responsibility usually devolves later, or even too late, to other people: anthropologists, sociologists, psychologists, philosophers, criminologists, or academics of all kinds. The problem is that there are not enough researchers in the human sciences capable of understanding the technological universe, and few among them have the ability to anticipate the impacts of these technologies. Moreover, even the criminologists, for example, can only proceed by reaction in respect to cybercrime. They only can analyze the consequences, document existing phenomena, and try to understand *a posteriori*, which means after the performance of criminal actions or deviant behaviours, how the new universe driven mostly by economical logic actually works.

3.7 Summary

Cybercriminality can affect everybody, from the oldest Internet user to the youngest, from the most naive to the best informed, and from the serious professional to the occasional leisure user. The ingenuity of the criminals is limitless. Nobody can be completely shielded from nuisances, scams, or criminal activities, be these frauds, spam, thefts, identity thefts, viruses, harassment, or excessive surveillance – to give just a few examples. The victims are frequently powerless in the face of this ubiquitous criminality. They suffer the consequences, knowing that any kind of legal comeback is generally an illusion.

Case study – From the FBI

Internet fraud investigation "Operation Cyber Loss"[42]

The FBI and Department of Justice are joined by the National White Collar Crime Center (NW3C) today to announce that criminal charges have been brought against approximately 90 individuals and companies as part of a nationwide series of investigations into Internet fraud, code named "Operation Cyber Loss," initiated by the Internet Fraud Complaint Center (IFCC). Subjects are facing a variety of Federal and state criminal charges which include fraud by wire, mail fraud, bank fraud, money laundering, and intellectual property right violations. The fraud schemes exposed as part of this Operation represent over 56,000 victims who suffered cumulative losses in excess of $117 million.

[42] Washington, D.C., 22 May 2001; FBI National Press Office (202) 324-3691.
http://www.fbi.gov/news/pressrel/press-releases/internet-fraud-investigation-operation-cyber-loss

Among the fraud schemes targeted are those involving on-line auction fraud, systemic non-delivery of merchandise purchased over the Internet, credit/debit card fraud, bank fraud, investment fraud, multi-level marketing and Ponzi/Pyramid schemes. Internet fraud can be defined as any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms, and e-mail, play a significant role in offering nonexistent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators. Many of these cases were initiated as a result of fraud complaints the IFCC received from individuals and businesses.

"Just as neighborhood watch programs keep watch over their neighborhoods and report suspicious activity to law enforcement, Internet users now have a 'cyber community watch' program. When individual citizens, businesses, and consumer agencies work with law enforcement at all levels, we help ensure the safety and security of the Internet," said Attorney General Ashcroft.

Director Louis J. Freeh stated, "The criminal charges being announced today demonstrate the critically important role that the IFCC plays in combating crime in cyber space. It is essential that law enforcement, e-commerce, and victims of crime have this electronic clearinghouse to expeditiously disseminate Internet fraud cases to the appropriate agency for investigation."

The IFCC became operational on May 8, 2000. The IFCC's mission is to address fraud committed over the Internet. For victims of Internet fraud, the IFCC provides a convenient and easy way to alert authorities of a suspected criminal or civil violation. Victims of Internet crime are able to go directly to the IFCC web-site at www.ifccfbi.gov, to submit their complaint information, relieving considerable frustration for them in trying to determine which law enforcement agency should receive their complaint. For law enforcement and regulatory agencies, the IFCC offers a central repository for complaints related to Internet fraud. All complaints are sent through an internal quality assurance process and are referred to the appropriate law enforcement and regulatory agencies. The IFCC uses the information to quantify fraud patterns, and provide timely statistical data of current fraud trends. The IFCC, located in Fairmont, WV, is a joint operation between the FBI and the National White Collar Crime Center (NW3C). It is the first project of its kind, a partnership between a federal law enforcement agency, and a non-profit private organization, serving Federal, state and local law enforcement agencies.

The accomplishments of this Operation are a direct result of the close working relationship law enforcement has developed with the private sector and e-commerce companies. As an example, Pay Pal, Inc. and Motley Fool have provided great assistance in identifying individuals engaged in wrong doing and reported that to the IFCC. The support and cooperation provided the FBI by other private sector companies such as Microsoft has also been instrumental in the success of Operation Cyber Loss.

"As the IFCC continues to expand its capabilities to better accommodate the needs of businesses, it has begun the work of creating the appropriate channels that will enable regular communication with representatives from the private-industry across the nation," said West Virginia State Auditor Glen B. Gainer III, chairman of the board of directors for the National White Collar Crime Center.

These cases have been coordinated by 28 FBI Field Offices along with participation by the U.S. Postal Inspectors Service; the Internal Revenue Service-Criminal Investigative Division; the Securities and Exchange Commission; U.S. Customs Service, the Competition Bureau in Canada; and numerous state and local law enforcement entities including the New York City Police Department; New Jersey State Police; Salt Lake City Police Department; Springville Police Department; Oregon High-Tech Team, the Oregon State Attorney's General Office; College Station, Texas, Police Department; Seattle Police Department; and the Monroe, Washington, Police Department; Boca Raton, Florida, Police Department; Florida State Comptrollers Office; Connecticut State Police; Chula Vista, California, Police Department; El Paso, Texas, Police Department; and the San Diego Police Department.

Questions

In respect to the case cited above: Internet fraud investigation – "Operation Cyber Loss":

Which needs are addressed by:

- the concept of "a cyber-community watch program"?
- the IFCC (Internet Fraud Complaint Center)?

What was the role of private entities in the resolution of this case?

Identify the major difficulties that needed to be overcome in resolving this case.

3.8 Exercices

1. How can cybercriminality affect personal dignity?
2. How can cybercriminality affect the physical and moral integrity of individuals?
3. In cyberspace, what are the factors exploited by certain predators to enable them to establish relationships with their victims?
4. Identify the major risky behaviours by Internet users that encourage cybercriminality.
5. Suggest arguments for the moral responsibility of communications service providers, particularly with respect to illicit contents.

6. What are the differences between the notions of cyberstalking and defamation on the Internet? What are their major impacts on their victims?
7. What are the characteristics of cyberbullying?
8. Give two examples of behaviours linked to the use of the Internet that could be considered unethical.
9. Why is Hate Speech considered a crime, both off-line as well as on the Internet?
10. Is it possible to have a global perspective on the realties of cybercrimes? Why?
11. Which are the factors or criteria necessary for the classification of cybercrimes?
12. How and why are "mules" recruited on the Internet? What is their responsibility?
13. Explain why identify theft is an important factor in cybercriminality.
14. Identify various methods or means that allow identity theft.
15. What are the most common types of fraud on the Internet?
16. Identify possible consequences of privacy offences of which an Internet user could be the victim.

Chapter 4

Cybercrimes Against Assets

4.1 Understanding the context

The Internet enables economic crime

As we have seen, cybercrime is the natural extension of ordinary criminal activity. Today, criminal acts are committed across cyberspace, separately from or alongside crimes.

Because of the networking of resources and individuals, cybercrime is highly effective. Not only companies, but also their information technologies and assets, can become attractive targets for criminal organizations in search of profit. This is a strategic threat to businesses, considering the fact that a business's assets can take the form of information rather then merely being physical items to be secured.

By opening the corporate gates to the Internet through web servers and communication services, enterprises expose themselves to the risks of attracting the attention of criminals and of giving criminals a potential foothold. While the Internet is a powerful communication tool, it is also a chaotic, dynamic, and hostile environment, which can be used to undermine an organization and serve as a vehicle for crime. The Internet can be seen as a high-crime zone. Given the importance that organizations attach to their online presence, and the growth of e-commerce activities, they are, in all likelihood, contributing to the expansion of criminality on the Internet.

Moreover, the Internet makes it easy to find and exploit new means of making money. This empowering feature is not, of course, lost on the criminal world. By embracing information technologies, criminals hope to increase their earnings while minimizing their exposure to risk. As it has done for many legitimate business activities, the Internet has empowered criminal ones. It offers performance, speed and a layer of isolation for carrying out criminal actions. These can be committed by individuals or small groups (the notion of disorganized crime) as well as by organized crime syndicates or mafias (Figure 4.1).

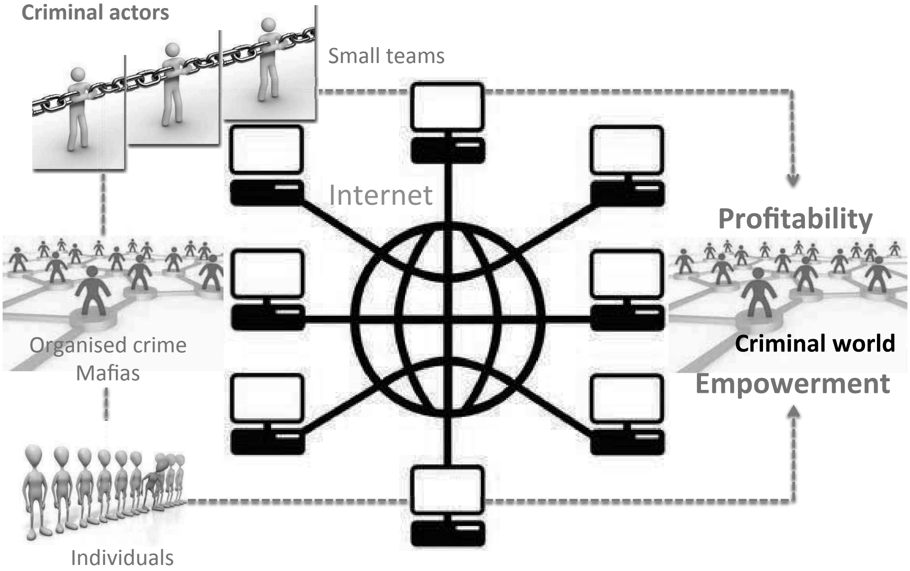


Figure 4.1 The convergence of criminal actors in cyberspace.

Economic crime not only affects large organizations. Individuals, organizations, and states can be hit by cyber economic crime activities with varying levels of nuisance and loss. Information and communication technologies allow isolated individuals to carry out economic crime activities at a distance and hidden behind a screen. They can either work alone or in concert with others, as organized virtual crime gangs of various sizes formed for a particular purpose or target. The information and software available on the Internet can bring together individuals, expertise, and tools and thereby facilitate cybercrime.

Furthermore, given the high degree of economic expertise and skills that economic crime sometimes requires, the Internet can facilitate preparations for, and the improvement of, cybercrime. Criminals can organize themselves around the access and exchange of information, thanks to the use of information technologies (acquisition of information about knowledge of markets, laws, technology, etc. that are needed to commit economic crimes). Internet resources can also be used to prospect for victims.

Economic crime is influenced by new technologies, which soon become part of the criminals' repertoire as they place information at the heart of their strategies and decision-making processes. Criminals exploit the speed, the relative anonymity, the dematerialization capacities and the facilities of the Internet in order to commit a large range of crimes. New technologies can facilitate theft of all kinds, tampering, information sabotage, and fraud. Blackmail, extortion, protection rackets, and ransom demands have all made the leap onto the Internet, as well as investment and auction fraud and other crimes.

Illustration from the FBI

> *Account Takeovers*
> Cyber criminals have demonstrated their abilities to exploit our online financial and market systems that interface with the Internet, such as the Automated Clearing House (ACH) systems, card payments, and market trades. In these instances, cyber crime is easily committed by exploiting the system users, rather than the systems themselves. This is typically done through the compromise of a legitimate user's account credentials.
>
> Fraudulent monetary transfers and counterfeiting of stored value cards are the most common result of exploits against financial institutions, payment processors, and merchants. While the losses that result from these exploits generally fall upon the financial institution, consumers experience the inconvenience of changing accounts and replacing cards associated with their compromised information, as well as the emotional impact associated with being a victim of a cyber crime.
>
> The FBI is currently investigating over 400 reported cases of corporate account takeovers in which cyber criminals have initiated unauthorized ACH and wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over $255 million and have resulted in the actual loss of approximately $85 million.
>
> Often, the attack vector is a targeted phishing e-mail that contains either an infected file or a link to an infected website. The e-mail recipient is generally a person within a targeted company who can initiate fund transfers on behalf of the business or another valid online banking credential account holder. Once the recipient opens the attachment or navigates to the website, malware is installed on the user's computer, which often includes a keylogging program that harvests the user's online banking credentials.

The criminal then either creates another account or directly initiates a funds transfer masquerading as the legitimate user. The stolen funds are often then transferred overseas. Victims of this type of scheme have included small and medium-sized business, local governments, school districts, and health care service providers.[1]

The consequences and direct costs for the individuals and organizations that fall victim to cybercrime are also borne by society, which suffers its impacts in an indirect manner. This could take the form of lost revenues, investment losses, or even job losses, as the examples below indicate.

Examples

In 2008, a Pennsylvania school district discovered that over $450,000 was missing from their bank account. The following year, a New York school district reported that approximately $3 million had been transferred out of their bank account. The New York's school district's bank was able to recover some of the transfers, but $500,000 had already been withdrawn from the account before the transaction could be reversed.

Recently, two trucking companies were victimized by fraudulent electronic account transfers, and lost approximately $115,000. Compared to some loss figures, this might not seem significant. One of the companies currently has annual revenues worth roughly $79 million, so their loss was nearly.1 percent of their gross revenue. That amount is approximately enough to purchase an additional tractor-trailer and provide another driver with a job.

In March 2010, an Illinois town was the victim of a cyber intrusion resulting in unauthorized ACH transfers totalling $100,000. When an authorized individual logged into the town's bank account, the individual was redirected to a site alerting her that the bank's website was experiencing technical difficulties. During this redirection, the criminal used the victim's authorized credentials to initiate transactions. The town was able to recover only $30,000.[2]

[1] Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation. Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit – Washington, D.C., 14 September 2011 http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

[2] Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation. Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit – Washington, D.C., 14 September 2011 http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

The Internet empowers organized crime

The various common forms of organized crime that are becoming increasingly sophisticated (protection rackets, human trafficking, confidence schemes, theft, etc.) can benefit from using new information technologies, in particular the Internet. Organized crime will tend to adopt the most advanced business practices, taking advantage of ICT and market characteristics to be efficient. With the communication facilities, the depersonalization of contacts, and the ease of access to data and to performance of transactions that it brings, the Internet can assist those engaged in any form of smuggling (whether it be of arms or human beings) and swindles (attacks against property, computer systems and infrastructure, data theft, copyright infringements, etc.).

The pursuit of profit is the main business objective of organized crime. So any legal or illegal tools and means, including violence, will be considered for the continuation of business. Internet provides an added element of competitiveness to organized crime. Cyberspace facilitates the search for criminal opportunities and targets and also the development of enterprises and activities. Organized crime is able to "hire" or to persuade legal, financial, or computer and security experts to work for it, by threats or by promised rewards.

From the press in 2004

> Crime syndicates and the Internet are a natural fit. Both are global, thrive on flexible networks and require specialization. The Net has allowed offshore gangs to branch into other ventures while devising new ways to commit old crimes, such as money laundering and counterfeiting. Criminals shop on illicit computer bulletin boards for stolen credit card numbers as they would for books on Amazon.com. They threaten devastating electronic attacks on Web sites unless they are paid. Online bank accounts are under siege. And millions of hijacked computers, or zombies – infected with malicious code under the control of a hacker without the owner's knowledge – perpetrate the schemes without a trail.[3]

Organized crime exploits the vulnerabilities of, and services provided by, the Internet, to gain access to private or public institutions or individuals. The Internet can be used for global outreach and search for potential victims, to prepare crimes, to commit crimes, or to manage logistics, for example. Economic crime (white collar crime) and organized crime (black collar crime) are

[3] Crooks slither into Net's shady nooks and crannies, By Jon Swartz, USA TODAY, 10/20/2004 http://www.usatoday.com/tech/news/2004-10-20-cyber-crime_x.htm

linked in many areas, and both use information and communication technologies to gain competitive advantages and be effective (Figure 4.2).

The pursuit of profits and the exploitation of the opportunities offered by markets, globalization and the Internet motivate economic and organized crime in the same way. In fact, organized crime invests a lot of money in technological innovations in order to use information and communication infrastructures to enhance their strategies, to be more productive for business-to-business exchanges, and for supply chain management, for example. Monitoring transactions, corporate espionage contributes to gaining competitive advantage over business rivals. Criminal organizations such as drug cartels, for example, exploit information and communications technologies to smuggle more drugs in a very efficient way, and have been doing this for a long time. From 1994, for example: "Colombian *cartels* have spent billions of dollars *to build one of the world's most sophisticated IT infrastructures*. It's helping them smuggle more dope than ever before."[4]

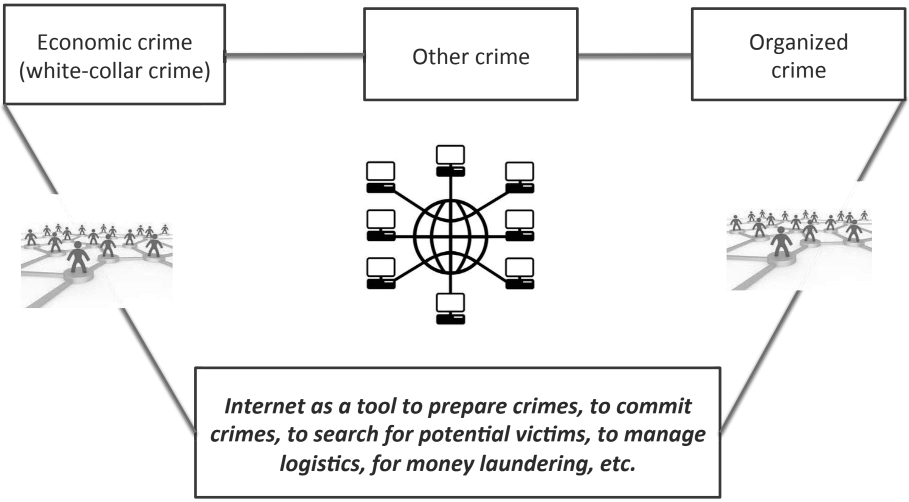

Economic crime (white-collar crime)
Other crime
Organized crime
Internet as a tool to prepare crimes, to commit crimes, to search for potential victims, to manage logistics, for money laundering, etc.

Figure 4.2 The Internet: a factor linking economic crime and organized crime, and the main activities within organized crime.

Another example was in 2000 when the Sicilian mafia, the Cosa Nostra, with some complicity from within the Banco di Sicilia, set up a massive online

[4] The technology secrets of cocaine inc. by Paul Kaihla, Business2.0; 4 July 2002 http://old.disinfo.com/archive/pages/news/id2352/pg1/index.html

banking fraud in order to subvert funds to the tune of 400 million U.S. dollars from a European Community fund destined to aid regional development. This fraud was not in the end successful, however, as informers notified the police.

Journalist Brian Krebs, who has reported on cybercrime for many years, described in his blog in July 2009[5] a case in which "Cyber criminals based in Ukraine stole $415,000 from the coffers of Bullitt County, Kentucky this week. The crooks were aided by more than two dozen co-conspirators in the United States, as well as a strain of malicious software capable of defeating online security measures put in place by many banks." This scheme was based on the sophisticated use of technology as well as personal contacts.

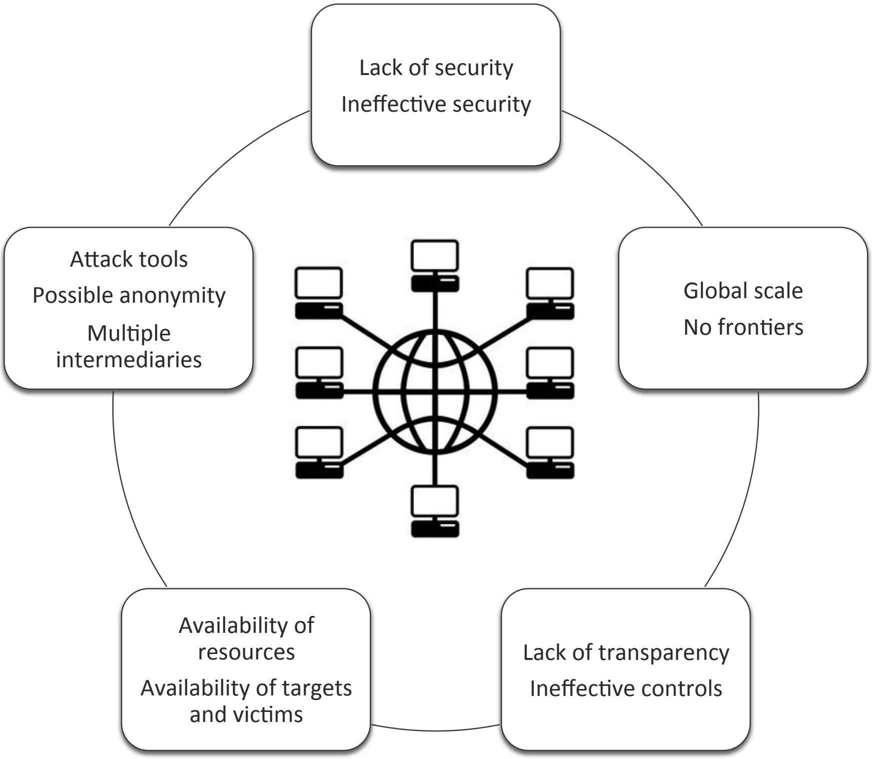


Figure 4.3 The main characteristics of the Internet that enable organized crime.

The global scale of the Internet makes it convenient for the transnational activities of organized crime. In addition, the culture of secrecy and the lack of transparency that are characteristic of organized crime strategy are well

[5] http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html

provided by the Internet. Activities are simplified by the capacity for anonymity, through the use of multiple technical intermediaries, by operating through cybercafés, and by covering up digital traces (Figure 4.3).

Furthermore, the Internet can permit the diversification of crimes, in particular in the financial sector. For example, disinformation and the manipulation of information, or the coersion and control of brokerage houses, can modify stock exchange prices and influence markets.

Money laundering

In the same way as all criminals who are exploiting the existing technical infrastructure, money-launderers are increasingly using the Internet in order to take money that has been generated by criminal activities such as drug trafficking, arms smuggling, corruption, prostitution, child abuse, and tax fraud, and launder it into legitimate funds.

Although it is greatly under-reported and frequently invisible, money-laundering via the Internet is increasingly popular. The Internet is an ideal vehicle for this, thanks to its virtual nature (anonymity, cyberspace, speed of transfer) and its freedom from territorial constraints (cross-border nature, conflicting competence and jurisdictions), which money-laundering agents have learned to exploit. The Internet makes it possible to channel money of criminal origins into legitimate economic activities using money transfers, investments, and capitalization.

Information and communication technologies will help considerably in concealing the origins of illegal money from taxation authorities. "Traditional underground banks, which have flourished in Asian countries for centuries, will enjoy even greater capacity through the use of telecommunications. The Asia-Pacific Secretariat of the Financial Action Task Force has advised that increased use of new technologies such as Internet banking and smart cards is making money laundering easier."[6]

Online investment, gambling, and commerce, such as the sale of imaginary goods and services for real money, make it possible to generate seemingly legitimate revenues that are difficult to monitor and almost impossible to prevent. E-banking, real-estate transactions via the net, the use of virtual front companies, and electronic cash can all be used to launder the proceeds of crime.

[6] Australian Institute of Technology.

Ordinary users may unknowingly support money-laundering when they use certain virtual services. Commercial organizations may also unwittingly become involved, with all the (potentially disastrous) implications that that entails, both legally and commercially. This is a major source of risk for companies.

Institutions involved in money laundering expose themselves to the following risks:

- risk of reputation (public image and trust): an institution associated with a money laundering business can suffer a significant deterioration of its image;
- legal risk: the discovery of money laundering operations can involve disciplinary sanctions;
- penal risk for the leaders and the employees.

With regard to the financing of terrorism by money laundering, the consequences can be more serious.

The money laundering process consists of all the techniques that transform illegitimate incomes produced by criminal activities into money which appears to be clean, in order to reinject it into legal economic and financial flows.

The money laundering process includes several phases:

Phase 1: The placement (preliminary wash). Criminals inject capital in legal circuits so as not to arouse any suspicion by:

- opening bank accounts;
- purchasing luxury products for example;
- purchasing stocks;
- games, betting, lotteries, etc.

Phase 2: The stacking (washing) consists in scrambling traces so that the origin of the funds is undetectable, and any traceability of the dirty money becomes complicated, if not impossible:

- multiplication of the movement of capital;
- transfers;
- transactions;
- successive withdrawals, etc.

Phase 3: The integration (drying): the money is ready to use without having to justify its origins. It will be used for purchases, investments or capitalization.

Information and communication technologies such as Internet services facilitate the concretization of these three stages of money laundering.

The following Internet services are frequently used in money laundering because there are no intermediaries, retail/credit operations are undetectable while being performed, and transfers are fast and safe:

- E-banking for electronic cloning (or *smurfing*): the criminal opens several bank accounts, under the same identity or different identities, splits his deposits, withdraws from and credits the accounts. Or criminals exchange amounts of money between themselves and nobody can establish a concrete link. Placement and stacking are carried out in peace.
- E-commerce facilitates virtual trade so a criminal can create a website selling fictitious products and/or services; the "virtual" company deals only with criminals and sells fictitious products and/or services, but payments are real.
- Games and virtual casinos: Online games offer the possibility of money laundering. From games on authorized websites, a criminal downloads ad hoc software, opens an account, obtains game credit, and plays. Money will be credited to the account.
- E-gold service offers an easy and anonymous facilities for opening accounts for the purchase and sale of gold on the Internet and for cash withdrawal everywhere in the world.
- Stock exchange websites that allow easy stock purchases on the Net by offering services for the receipt, transmission, or execution of Stock Exchange orders. These services benefit the specialists laundering money.
- Electronic coin holders are increasingly being used for money laundering.
- Currently there are few effective means of controlling the phenomenon of IT-enabled money-laundering.

4.2 The typology of the main crimes against assets

Economic crime activities can be categorized with respect to the laws that define them. In general, the categories of economic cybercrime shown in Figure 4.4 are largely recognized at an international level.

Theft of resources or services

The Internet not only provides the ideal conditions for new illegal projects and activities, but also makes variations on fraud and other crimes possible by means of computers. The theft of services and infrastructure resources (processor time, storage, etc.) is defined as the use of services with the intent to avoid payment for those services.

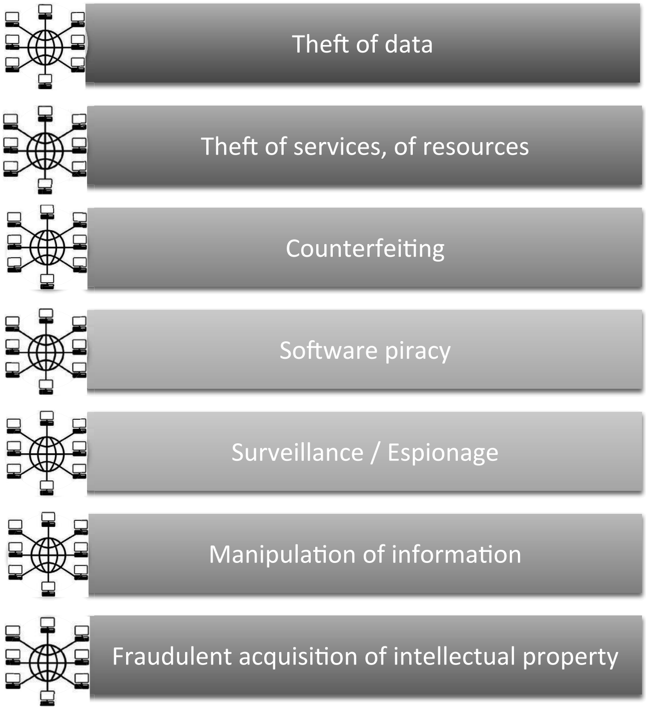

Theft of data
Theft of services, of resources
Counterfeiting
Software piracy
Surveillance / Espionage
Manipulation of information
Fraudulent acquisition of intellectual property

Figure 4.4 The main cybercrimes related to economic crime – cybercrimes against assets.

Thefts of telecommunications services account for some of the greatest economic losses experienced by telecommunications operators. Telecommunication infrastructures are high priority targets for criminals. Once fraudsters have accessed the switchboard and gained access to the PBX (Private Branch eXchange – telecommunication switch) by stealing identities and access codes, they can have access to dial-in/dial-out circuits. This provides free calls and call time, which can be sold and thus used to generate profits as illustrated by the two following examples.

In 2000, a computer engineer was accused of stealing 100 hours of Internet time from a client. Hackers boast of accessing the customer accounts of a country's Internet Service Provider, and of using them freely. In 2004, suspects were arrested on charges of illegally hacking the systems of a country's long distance telephone company since 1998. They hacked the telephone network and sold call time. The company reported a financial loss of £1.9 million during those six years.[7]

[7] Adapted from www.news.zdnet.co.uk

From the FBI

Federal Bureau of Investigation (FBI), Miami Field Office, announce the indictment of nine defendants for their participation in the theft of 5,250 Toshiba laptop computers, valued at approximately $1.9 million, which were being shipped from Forest Park, Georgia to Miami, Florida in July 2010.[8]

Illustration

Telecommunication Network Disruption

Financial networks are highly dependent on the availability of telecommunication infrastructure. Although cyber criminals may not be able to directly target the core processing centers that support the critical financial markets, they may target the telecommunication networks to directly impact the functionality of key financial players.

In market trading, infrastructure is crucial to the success of firms that specialize in high-frequency trading as milliseconds of saved time during data processing and transmission can impact profits. As a result, many firms co-locate and buy space near the main processing center of the major exchanges. The close proximity of these networks adds a shared reliance on telecommunication infrastructures, which could be significant if there is a disruption to the infrastructure.[9]

The theft of IT equipment, notably of laptop computers in public places (such as stations, hotels or airports) is very common. These thefts can be directly targeted at business executives with the intention of carrying out business espionage and can lead to the theft of strategic information, secrets, intellectual property, or even personal data or photos that could prove embarrassing for their owner. These data could be the basis for leverage, blackmail, or extortion.

In other cases, online frauds can lead to the theft of IT equipment, as the case below illustrates.

From the press

In one of the largest Internet fraud investigations, the FBI and international law-enforcement authorities in August 2004 obtained a federal grand-jury indictment of a suspected Romanian computer hacker and five Americans on charges they conspired to steal more than $10 million in computer equipment from distributor

[8] http://www.fbi.gov/miami/press-releases/2011/nine-indicted-in-1.9-million-theft-of-laptop-computers

[9] http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

Ingram Micro in Santa Ana, Calif. The indictment charges that C. M., 24, using the alias Dr. Mengele, hacked into Ingram's online ordering system and placed fraudulent orders for computer equipment. The order directed the equipment be sent to dozens of addresses throughout the USA."[10]

Theft of data

Thefts of data (database records or files), or sensitive information (passwords, social security numbers, medical records, secrets, intelligence information, or classified information) can easily be carried out using information and communication technologies. Data can be intercepted during transmission or accessed when stored. This can contribute to white-collar crimes in various ways.

Example

In 2003, a hacker was arrested for gathering personal information and transferring cash into his personal account. This employee of a country bank used the closed-circuit television cameras (CCTV – used for surveillance) to intercept client data such as passwords by recording the keys pressed.

Another common scam consists of announcing to recipients that they have won a holiday trip for two people. Typically in order to get their jackpot, victims have to fill out some forms and provide some credentials, such as banking details and ID numbers, that could then be used by criminals for further transactions.

From the FBI

Hacker Pleads Guilty to Infiltrating AT&T Servers, iPad Data Breach – *Defendant Stole E-Mail Addresses and Personal Information Belonging to 120,000 Apple iPad 3G Subscribers*. A computer hacker (D.S) who helped write the malicious code behind a breach of AT&T's computer servers admitted today to conspiring to hack into the servers, steal information regarding iPad subscribers, and publicize the crime.

D. S. admitted that he was a member of an organization known as Goatse Security, which, according to its website, is a loose association of Internet hackers and

[10] Jon Swartz, USA TODAY. 10/21/2004. http://www.usatoday.com/tech/news/2004-10-20-cyber-crime_x.htm

self-professed Internet “trolls” – people who intentionally, and without authorization, disrupt services and content on the Internet.

Prior to mid-June 2010, AT&T automatically linked an iPad 3G user’s e-mail address to the Integrated Circuit Card Identifier (“ICC-ID”), a number unique to the user’s iPad, when the user registered. As a result, every time a user accessed the AT&T website, his or her ICC-ID was recognized and his or her e-mail address was automatically populated for faster, user-friendly access to the site. AT&T kept the ICC-IDs and associated e-mail addresses confidential.

Seeing this, and discovering that each ICC-ID was connected to an iPad 3G user e-mail address, hackers, including D.S., wrote a script termed the “iPad 3G Account Slurper” and deployed it against AT&T’s servers.

The Account Slurper attacked AT&T’s servers for several days in early June 2010, and was designed to harvest as many ICC-ID/e-mail address pairings as possible. It worked by mimicking the behavior of an iPad 3G so that AT&T’s servers would be fooled into granting the Account Slurper access. Once deployed, the Account Slurper used a process known as a “brute force” attack – an iterative process used to obtain information from a computer system – against the servers, randomly guessing at ranges of ICC-IDs. An incorrect guess was met with no additional information, while a correct guess was rewarded with an ICC-ID/e-mail pairing for a specific, identifiable iPad 3G user.

D. S. admitted to communicating during the data breach with his co-defendant, A. A. who was arrested January 18, 2011, in Fayetteville, Ark., while appearing in state court on unrelated drug charges. The two wrote each other during the breach using Internet Relay Chat, an Internet instant messaging program. Those chats included discussions between D.S., A.A., and other Goatse Security members about the best way to take advantage of the breach and associated theft.

Immediately following the theft, the hacker-authors of the Account Slurper provided the stolen e-mail addresses and ICC-IDs to the website Gawker, which published the stolen information in redacted form, along with an article concerning the breach. The article indicated that the breach “exposed the most exclusive e-mail list on the planet,” and named a number of famous individuals whose e-mails had been compromised […] On June 10, 2010, immediately after publicizing the breach, D.S. and A.A. discussed destroying evidence of their crime.”[11]

The case gained national attention because the stolen e-mail addresses included those of members of the Senate and the House of Representatives, and employees of the Justice Department, NASA and the Department of Homeland Security. There were also a number of celebrities on the list. Mr. A.A. passed the information along to the gossip blog Gawker.[12]

[11] http://www.fbi.gov/newark/press-releases/2011/hacker-pleads-guilty-to-infiltrating-at-t-servers-ipad-data-breach
U.S. Attorney’s Office June 23, 2011 – District of New Jersey (973) 645-2700.

[12] http://bits.blogs.nytimes.com/2011/06/23/guilty-plea-in-theft-of-data-on-ipad-owners/

The theft of electronic data can be performed by those people who are in the habit of accessing and using those data for legitimate professional purposes. In many organizations, including banks and insurance companies, staff with specific technical and business skills will be employed to perform all kinds of data analysis, looking for patterns of transactions, loads on systems and applications, instances of fraud, examples of the failure of internal controls, and many other indicators or items of information of interest to the management of the organization. In order to perform this kind of analysis, the staff will often have access to quantities of current and sensitive data and the tools necessary to manipulate and convert the data. Once the data have been extracted from central systems and are sitting in files on a desktop or a network, there are vulnerable to disclosure, both accidental and deliberate.

Illustration

HSBC admits huge Swiss bank data theft

About 24,000 clients of HSBC's private banking operation in Switzerland had personal details stolen by a former employee, the company has admitted. […] The information stolen concerns 15,000 accounts that are still active. Another 9,000 accounts have been closed since the theft.

[…] About 24,000 clients of HSBC's private banking operation in Switzerland had personal details stolen by a former employee, the company has admitted. […] The former employee, H.F., who worked in HSBC's IT division, fled to France while under investigation in Switzerland.[13]

Surveillance, espionage and information manipulation

Industrial espionage may take a number of forms, such as information theft, social engineering, wiretapping, or unauthorized access to classified or proprietary information. It could be directed against companies or governments, in order to take competitive advantage or economic gain.

Example

Some examples of malicious software, such as "Poker Viewer," aim to wiretap game information. During an online poker game, a player is not able to see his opponent's cards, but Poker Viewer can be used to intercept information from the game server, allowing the player to see his opponent's hand. When created in 2001,

[13] http://news.bbc.co.uk/2/hi/business/8562381.stm

the main objective of Poker Viewer was to exchange online money for cash. Illegal profits were made by selling accounts to users. The software was then adapted to intercept information from the server and was sold to online players. Huge profits were made from these frauds. Thirteen people were arrested.[14]

Software piracy, the fraudulent acquisition of intellectual property, and counterfeiting

The ease with which digital information can be reproduced has spawned a market for illegal copies. A great variety of intellectual property infractions is possible: forging an author's work (including software), copying designs, copying models, or infringing trademarks.

The illegal downloading of software, music or movies – whatever technology is used (peer-to–peer, etc.) – is the most common form of Internet related crime. The emerging national laws that criminalize this kind of behavior raise the question of the free circulation of cultural assets, knowledge, and ideas. This is partly linked to political, economic, and ideological issues related to the definition of crime and partly to intellectual property and copyright.

Piracy is the act of violation of copyright. It can take several forms in cyberspace: unauthorized copies, or the distribution or sale of copyright material that may or may not be counterfeit (copyright thieves) over which some other party claims to possess proprietary rights.

Counterfeiting refers to informational goods infringing copyright by replicating the original product in terms of appearance, and thus being passed off as authorized copies.[15]

Piracy has several negative economic impacts, including loss of market share, tax revenues, or jobs. At the same, piracy can be argued to allow individuals to have access to computer resources and services that they cannot afford if they had to pay for them. However this fact can contribute in particular contexts to reducing the digital divide.

Intellectual property theft is a long-existing crime related to the fraudulent acquisition of someone else's ideas, inventions, or creative expressions. It can be related to trade secrets or to specific digital contents protected by copyright, such as music, films or software. Software piracy includes the unauthorized copying or distribution of copyrighted software.

[14] www.sophos.com

[15] The rate of piracy by region can be found in the annual BSA Global Piracy Study. According to the Business Software Alliance, software worth 59 billion U.S. dollars was stolen in 2010. www.bsa.org/globalstudy/

In some cases it could involve the circulation of counterfeit products. The sale of counterfeit products on the Internet, most notably through auction sites, forms a significant criminal activity. When the products in question are pharmaceuticals, quite apart from the financial impact on the genuine pharmaceutical companies, this trade can have serious effects on the health of the people who purchase and consume the products. Similar to a club-goer who buys illegal drugs from a dealer in the street, the purchaser of counterfeit pharmaceuticals over the Internet cannot know the provenance or the content of the medication.

4.3 Frauds and scams

Nigerian scam, Nigerian letter (also called 419 fraud)

The Nigerian scam, a clever and dishonest plan for making money, consists of an unsolicited email originally sent from Nigeria, hence the name. Several variations of the advance fee scheme exist and are no longer only issued from Nigeria[16]. The Nigerian letter is an old fraud that is also carried out by letter or fax, but nowadays electronic mail has made it very efficient by offering the opportunity to reach an impressive number of potential victims at a very low cost. Lists of valid email addresses can be bought for a small amount of money.

The contents of the mail typically promise a huge amount of money in exchange for a small advance payment and bank account information; usually the victim is asked to assist with a particular financial transaction, such as placing funds in overseas bank accounts or the remote payment of taxes. Examples of 419 email scams include a message claiming to come from a persecuted widow of the late Nigerian head of state, an associate of the massacred Nepalese royal family, and even an African astronaut stranded on the Mir space station.

As an example of a classic scenario, in January 2006, some Internet users were bombarded with emails supposedly sent by the personal secretary of billionaire Mr. Nobody, who was chief executive officer of a national oil company. The emails offered the recipient USD 10 million in exchange for assisting in the transfer of USD 45 million, a part of Mr. Nobody's fortune. Emails were used to steal confidential information, such as bank account numbers, so

[16] The Nigerian letter is also named 419 fraud because of the violation of Section 419 of the Nigerian Criminal Code.

that the criminals could later steal money and commit identity fraud with the data they had gathered.

The criminals involved in these schemes have limitless imaginations. They can modify their bait in the light of any events that are in the headlines, such as the earthquake in Haiti or a transport disaster. When confronted by appeals for donations and requests for charitable assistance, through email messages and websites, the Internet user always has to remain vigilant (Figure 4.5).

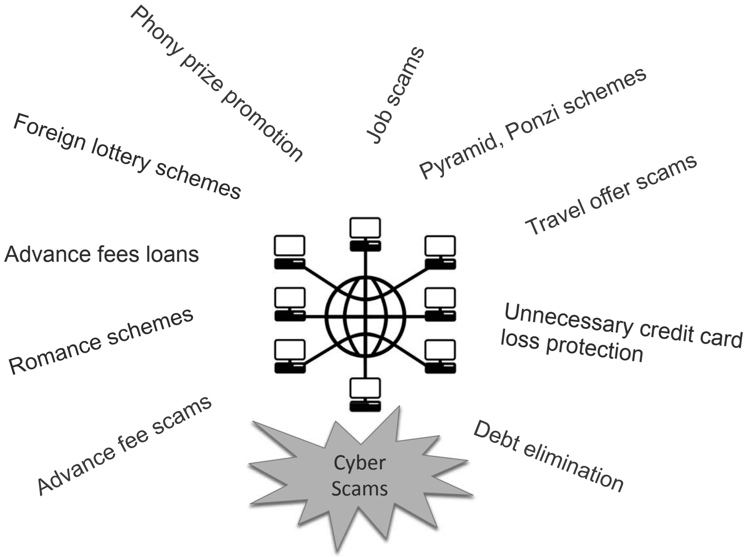


Figure 4.5 Some examples of scams.

From CNN

FBI warning of Haiti earthquake scams

As the world looks for ways to help the victims of Haiti's earthquake, the FBI is now warning that there are also those who are looking for opportunities to set up scams surrounding the latest disaster relief efforts. The FBI advises that people should be very skeptical of any unsolicited appeals they receive or find on the Internet. One month after Hurricane Katrina, the FBI said it was suspicious of most of the 4,600 Web sites soliciting money on behalf of those victims. Within an hour of the World Trade Center attacks, scam sites popped up on the Web according to ScamBusters.org.[17]

[17] CNN, Linda Petty; 13 January 2010 http://articles.cnn.com/2010-01-13/living/haiti.charity.scams_1_charity-web-sites-fbi?_s=PM:LIVING

There exist a number of variations on the theme of the Nigerian Letter; all are frauds. They are particularly widespread nowadays because of the fact that fraudsters can act while remotely hidden behind a screen and not face-to-face, thus increasing their range and minimizing the risk of being identified.

In the following sections we will discuss a number of typical types of cyberfrauds.

Blackmail and cyberextortion

Information resources may in effect become potential hostages of cybercriminals. Blackmailers have shifted their operations to cyberspace, and anyone may suddenly find themselves the victim of attempts at blackmail, spreading disinformation, or disseminating propaganda. Furthermore, the explosion in identity theft since 2003 has shown that the benefits of anonymity that the Internet affords, and the use of false identities to avoid prosecution or the attribution of criminal responsibility for actions, have not been lost on criminals. Identity theft, readily performed via the Internet, is a factor in illicit activities.

Internet extortion often involves hacking into and controlling computer resources (such as database, servers, or files), promising to release control back to the company if funds are received or if specific people are employed in technical roles. At the same time, the perpetrators may threaten to destroy information or make it public.

A real-life example

The vice president of an IT company hired two well-known hackers via IRC to hack the websites of some of his company's clients. The objective of the attack was to gain administrator rights to these sites. The VP then asked the hackers to find and analyze security loopholes in the online presence of what amounted to 180 small and medium-sized companies. Once the vulnerabilities were found, the IT company reported them to the businesses in question and suggested that they buy security consulting services from the company in order to find suitable security counter-measures.

Cybercriminals can blackmail their victims by threatening to make their IT infrastructures unavailable, to publish certain information, or to take control of certain resources. They can also seize control of the resources and demand payment in return for returning that control to the business. The amounts of money in question in such activities is variable and depends on the importance to the organization of the people and resources in question and the scale of the attack, but can reach considerable sums.

Cyberextortion can now be classed alongside spam and other types of cyberattacks as key tools for cybercriminals. A large number of cases of cyberextortion, attempted or successful, are not reported for reasons that could be related to the futility of doing so or the fear of negative publicity.

This kind of threat can be implemented by, for example:

- denial-of-service attacks to leave resources, services, data or processes unavailable;
- use of software known as "ransomware" which can, for example, encrypt the target's data against the owner's wishes, with the decryption key provided after payment is made;
- takeover of control of resources through the installation of a Trojan horse;
- manipulation of opinion, affecting the reputation of the business.

The following case illustrates the last of these possibilities.

Illustration from the FBI

Manhattan U.S. Attorney Charges California Man with Cyber-Extortion of New York-Based Insurance Company

A. D. was arrested on March 6, 2010, on charges of attempting to extort approximately $200,000 from a New York-based life insurance company by threatening to make false public statements and transmit computer spam in an effort to damage the reputation of the company and cost it millions of dollars in revenue

[…] According to a criminal complaint unsealed on March 8, 2010, in Manhattan federal court:

On February 22, 2010, more than a dozen employees, executives, and one board member of the life insurance company (the "Company") received an e-mail […] The e-mail reads, in part, "I HIGHLY suggest you visit this website and contact me afterwards." The e-mail provides a website address that leads a viewer to a website created by A. D. (the "Website").

The website includes, among other things, the following text:

a. These things, unless you honor the below claim, WILL HAPPEN on March 8, 2010.
b. As you have denied my claim I can only respond in this way. You no longer have a choice in the matter, unless of course you want me to continue with this outlined plan. I have nothing to lose, you have everything to lose.
c. My demand is now for $198,303.88. This amount is NOT negotiable, you had your chance to make me an offer, now I call the shots.

d. I have 6 MILLION e-mails going out to couples with children age 25-40, this e-mail campaign is ordered and paid for. 2 million go out on the 8th and every two days 2 million more for three weeks rotating the list. Of course it is spam, I hired a spam service, I could care less, The damge [sic] will be done.
e. I am a huge social networker, and I am highly experienced. 200,000 people will be directly contacted by me through social networks, slamming your integrity and directing them to this website within days.
f. I think you get the idea, I am going to drag your company name and reputation, through the muddiest waters imaginable. This will cost you millions in lost revenues, trust and credibility not to mention the advertising you will be buying to counter mine. Sad thing is it's almost free for me!
g. The process is in motion and will be released on March 8th, 2010. If you delay and the site goes live, The price will then be $3,000,000.00…[18]

In contrast to the previous example, in the following case, the amount demanded was not great. However, the large number of victims targeted by the attack ensured that it would be profitable.

From the news

Russia-based child porn scam hijacks PCs
Users are exhorted to pay a ransom fee or be reported to police

Russian cybercriminals have launched a vicious new scam that uses the threat of child pornography to hijack victims' computers until they pay a ransom fee.

The scam spreads via a Trojan hidden in "innocent-seeming links" on social networking sites and in emails. Once the rigged link is clicked on, the Trojan penetrates the computer and alerts the user that child pornography has been found on the system. That's only part of the problem; the Trojan doesn't simply warn the victim, it effectively hijacks their computer, displaying a message that takes up 90 percent of the screen and prevents the operating system from running properly […] To eradicate what they now believe is child porn and to regain control of their computers, victims are prompted to pay the con artists about $17 within 12 hours, or they will be reported to the police and all their computer's data will be blocked or deleted. Although the bait in this scam is particularly nasty, the structure of it follows the form of nearly all "scareware" exploits, in which victims are pressured, usually through fear of computer failure, into purchasing software they don't need.[19]

[18] FBI, The New York Fiel Office. U.S. Attorney's Office March 08, 2010 – Southern District of New York
http://www.fbi.gov/newyork/press-releases/2010/nyfo030810.htm

[19] Matt Liebowitz, 9/6/2011
http://www.msnbc.msn.com/id/44416129/ns/technology_and_science-security/#.Tx6skE_thaT

There exist a number of different ways of extorting money. Apart from messages or software that can be classed as ransomware, there are messages that relate to malicious advertising (or “malvertising”) and fraud that play on users’ fears. Often these cases consist of a security pop-up window that informs the users that their machines are vulnerable to cyberattacks or have been infected. These are examples of “scareware” that can be more or less aggressive and which can sometimes be very difficult to remove or work around. Typically they imitate pieces of software or messages coming from legitimate, genuine security organisations. They offer security solutions that are at best inactive and at worst install malware themselves (viruses, Trojan Horses, spyware) that can subsequently be used for the theft of data, for identity theft, for carrying out fraudulent financial transactions, or for taking control of the computer remotely with the intention of using it as a zombie machine within a botnet.

While surfing on the web, the Internet user can also be drawn into clicking on adverts for security products and services that are themselves fraudulent.

The financial consequences of these attacks can include direct access to the victim’s bank account (for the withdrawal or transfer of money) or more indirect consequences, such as the costs of cleaning and repairing an infected machine. Such attacks can also give rise to forms of extortion to the extent that the Internet user purchases a security solution that is never provided. Within the general category of cyberextortion fall the frauds related to lottery wins that are based on the following principle:

Extortion by lotteries scheme

“This is to inform you of the release of monetary winnings to you. Your email was randomly selected. You have earned 1 million dollars. Please contact […] An initial fee is requested to initiate the process […]” In general, this initial fee will range from 1,000 to 5,000 U.S. dollars. Additional fees are then requested after the first payment.

Those who reply to such messages and get involved in these frauds often have great difficulties in getting out of them and are led into paying considerable sums before realising that they have fallen victim to thefts and then taking the necessary steps to report the circunstances to the police to obtain help. Sometimes victims have borrowed money or even stolen from those around them in order to produce the sums demanded. There have even been cases of people taking their own lives out of a sense of shame at having been conned or to avoid the legal consequences of their actions, especially when they have been incited to perform criminal acts at the behest of the criminals behind the frauds.

Cybercriminals exploit current affairs to create plausible schemes and draw in a maximum number of naïve victims. As an example, in 2004, as soon as South Africa was awarded the 2010 FIFA World Cup, the following scheme, that combines several means of distribution, saw the light of day:

> In 2004, scam letters were sent to mailboxes. These emails, called "SA 2020 World Cup Bid Lottery," announced to the recipient that he had won the lottery. This happened a few days after the country was selected to host the 2010 World Cup. After receiving a certificate confirming their prize, the recipients were asked to give some personal information. Then, the victim was requested to deposit a certain amount of money that went as high as USD 49,233, for attorney's fees and clearances in order to transfer the lottery money. The investigation counted 81 victims of this lottery scam. Some fraudsters used the national lottery to steal personal information. They pretended to have tips to win at the lottery and asked recipients to join them. In exchange for discovering these tips, victims had to pay exorbitant membership fees.[20]

Investment fraud and other financial frauds

An investment fraud is an offer using false or fraudulent claims to solicit investments or loans, or providing for the purchase, use, or trade of forged or counterfeit securities. The Internet enables *investment fraud* by information manipulation and distortion. Some are known as Ponzi or pyramid schemes. Ponzi schemes are investment scams in which investors are promised abnormally high profits on their investments. No investment is actually made. Early investors are paid returns with the investment money received from the later investors. The system usually collapses. The later investors do not receive dividends and lose their initial investment.

Figure 4.6 presents some examples of financial frauds occurring over the Internet that take advantage of the global scale of information and communication activities.

[20] www.sophos.com

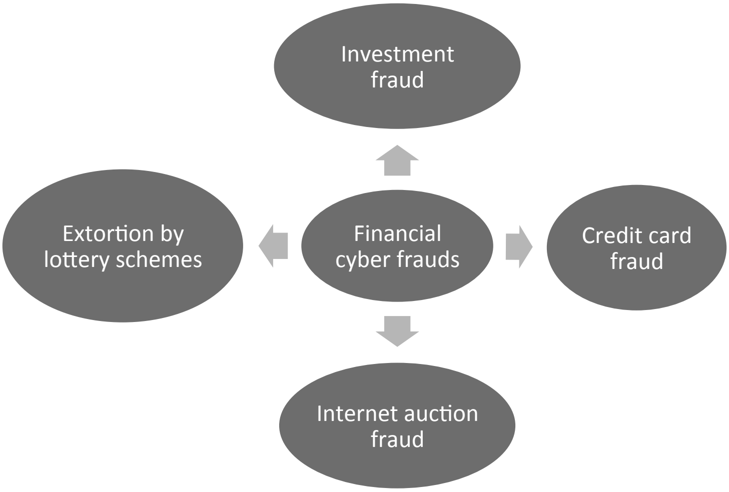


Figure 4.6 Some well-known financial cyberfrauds.

Example adapted from a real case

In a country, two fraudsters were arrested after hacking a computer system and stealing a stock company's account information. They first hacked about 20 accounts and sold the stocks from these accounts. Then, they bought their own stocks at a high price using KOSDAQ stocks to maximize their benefits. The two fraudsters are accused of "illegal acquisition of property."[21]

Credit card fraud

Credit card fraud concerns the use of fraudulent credit cards or the unauthorized use of a credit/debit card or card number to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured websites, or can be obtained in an identity theft scheme.

Example adapted from a real case

An ex-private lender created a website using a stolen identity. The former lender reached other lenders by phone and tempted them to become members of his new website. He succeeded in attracting 2,736 private lenders, and

[21] www.ctrc.go.kr

thus gathered the personal information of 20,486 borrowers. The membership allowed the lender to check the credit situation of each borrower before loaning them money. Besides online information, private lenders also received information on their mobile phones as soon as a borrower with a classification in the "Red" zone, that is to say having a low credit level, asked for a loan. Both of these consultations of personal and confidential information were totally illegal in the jurisdiction in question. The police investigation showed that the suspect earned a large amount of money from membership fees. During the same year in the same country, suspects who managed a loan office used the personal information of their clients to register on websites and purchase untraceable mobile phones and credit card terminals. The suspects made at least 319 fraudulent airline tickets purchases to launder the illegal cash and profits gained through the illegal use of credit cards and their illegal personal loan business.

Internet auction fraud

Auction fraud involves fraud in connection with the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through such a site (Figure 4.7).

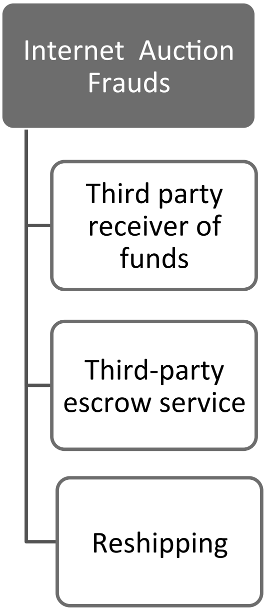


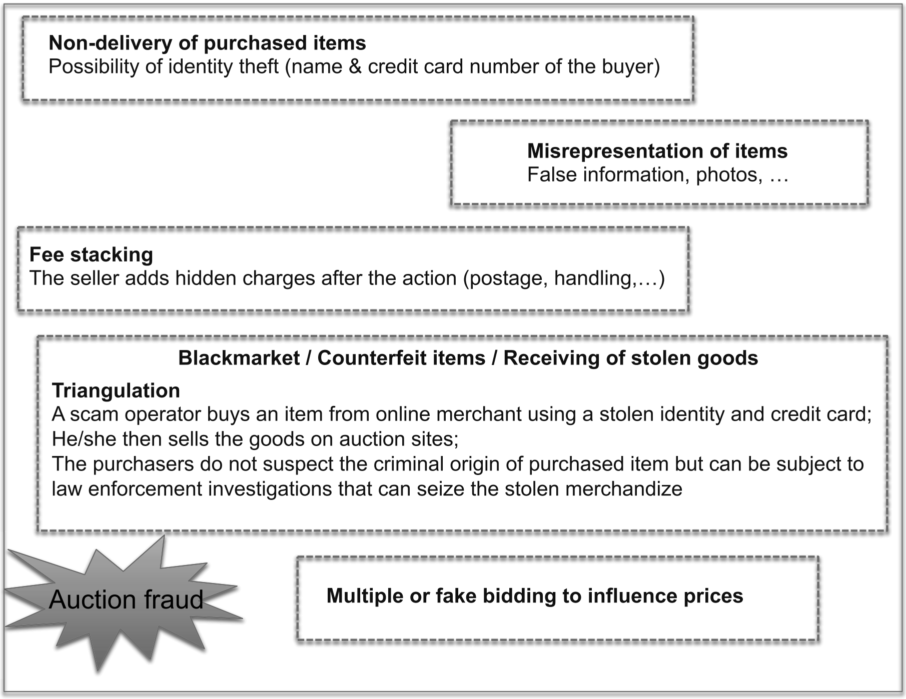
Figure 4.7 Types of Internet action frauds.

Example adapted from a real case

On several well-known auction sites, computers and digital cameras were advertised. The total sales amounted to a large sum of money deposited in many bank accounts. Purchasers – 220 of them – were spread over 11 countries, and 55 of them reported not having received any goods. The investigation allowed the identification and apprehension of 20 individuals who were the owners of the bank accounts in question. The auction sites were pleased to remove these advertisements, and the bank closed the related bank accounts. Some variants of auction fraud exist and are commonly grouped together as the third party receiver of funds, third-party escrow service, or reshipping.

Third party receiver of funds

Internet auctions are posted on auction websites by a criminal seller who also proposes work-at-home jobs on Internet employment sites in which he solicits assistance in receiving funds from auction sales, claiming that he cannot directly handle the remittances as a result of his location overseas. The



Non-delivery of purchased items
Possibility of identity theft (name & credit card number of the buyer)

Misrepresentation of items
False information, photos, …

Fee stacking
The seller adds hidden charges after the action (postage, handling,…)

Blackmarket / Counterfeit items / Receiving of stolen goods

Triangulation
A scam operator buys an item from online merchant using a stolen identity and credit card;
He/she then sells the goods on auction sites;
The purchasers do not suspect the criminal origin of purchased item but can be subject to law enforcement investigations that can seize the stolen merchandize

Multiple or fake bidding to influence prices

Figure 4.8 Examples of Internet action frauds.

criminal seller asks the individual to act as a third party receiver of funds from victims who have purchased products (that do not exist, a fact of which they are unaware) via the Internet. The victim, receiving the funds from the purchasers, then wires the money to the organiser of the fraud. This scheme makes it very difficult to identify and catch the fraudulent individual (Figure 4.8).

The *reshipping method* is similar to a third-party scheme. It entices intermediaries ("reshippers") to receive merchandise at their home, for repackaging and sending on to criminals. In doing so, the reshippers, without knowing it, facilitate the transfer of goods purchased online by fraudulent means such as stolen credit cards. Often they are recruited through Internet Relay Chat, through employment offers for working at home, or even over the phone. They can be paid in kind by being allowed to keep some of the merchandise.

Example from news.cnet.com

> *RSA reveals details behind re-shipping scam*
>
> RSA FraudAction Research Lab has uncovered the workings behind a recent re-shipping scam in which U.S. residents were used as mules to send goods purchased with stolen credit card numbers overseas. The operation began a year ago and received applications from more than 1,900 people, though only 33 people were "hired," according to an RSA FraudAction Research Lab. Laptops, iPods, iPhones, Nokia smartphones, digital cameras, Sony PlayStation 3 devices, and DJ equipment were among the items shipped to addresses in Russia and Belarus. RSA estimates that more than $36,000 worth of merchandise was cashed out every month before the scam ended earlier this year. The operation masqueraded as a company called "Air Parcel Express," and it had an authentic-looking Web site, RSA said. However, there is a legitimate shipping firm with the same name that is completely unassociated with the scam. The use of unwitting accomplices to re-ship items purchased fraudulently in the U.S. to other countries is not new. However, the degree to which the scammers went in creating the illusion of legitimacy is noteworthy, RSA said.
>
> "They had a really professional, highly executed effort in recruiting the re-shippers, which is fairly novel," said S. B., senior manager of identity protection and verification at RSA. "The average re-shipping campaign is based on e-mail or ads that direct people to a crude location" on the Web, he added.
>
> Here's how the scams work. Criminals get credit card numbers through phishing, Trojan attacks, and hacking databases, like that of Heartland Payment Systems and RBS WorldPay. They use the information to make online purchases of items, typically electronics goods that they can resell at a high profit and typically purchased in the U.S., where they are cheaper. The criminals recruit U.S. residents to receive and re-ship the goods out. Re-shippers are asked to unpack the item from the merchant's box and put it in a plain box, probably so the boxes face less scrutiny at customs, Brady said. To find the mules, the criminals advertise on legitimate

> employment Web sites and on search engines. Usually, the re-shippers don't get paid as promised, RSA said. "What's interesting is that criminals in Eastern Europe can orchestrate the campaign, recruit in the U.S., and ship to Europe without ever needing to have any level of personal contact" with the re-shippers, S. B said.[22]

Escrow service fraud scheme

A criminal will propose the use of a third-party escrow service to facilitate the exchange of money and merchandise. The victim is unaware that the criminal has actually compromised a legitimate escrow site and, in reality, created one that closely resembles the legitimate escrow service. The victim sends payment to the phony escrow provider and receives nothing in return. Alternatively, the victim sends merchandise to the criminal subject and waits in vain for his payment through the escrow site; this payment is never received because it is not a legitimate service.

Click fraud

Click cyberfrauds are specific to some e-marketing applications and to pay-per-click online advertizing services. When a user clicks on an online advertisement, it generates a charge. Some criminals divert this mechanism and manipulate the system to their advantage by generating illegitimate clicks.

Illustration from Bloomberg BusinessWeek

> *Click Fraud – The dark side of online advertising*
> M. F. put his faith in online advertising. He used it to build his Atlanta company, MostChoice.com, which offers consumers rate quotes and other information on insurance and mortgages. Last year he paid Yahoo! Inc. (YHOO) and Google Inc. (GOOG) a total of $2 million in advertising fees. The 40-year-old entrepreneur believed the celebrated promise of Internet marketing: You pay only when prospective customers click on your ads.
> Now, M.F,'s faith has been shaken. Over the past three years, he has noticed a growing number of puzzling clicks coming from such places as Botswana, Mongolia, and Syria. This seemed strange, since MostChoice steers customers to insurance and mortgage brokers only in the U.S. Fleischmann, who has an economics degree from Yale University and an MBA from Wharton, has used specially designed software to discover that the MostChoice ads being clicked from distant shores had appeared not on pages of Google or Yahoo but on curious Web sites with names

[22] Elinor Mills, 12 November 2009
http://news.cnet.com/8301-27080_3-10396478-245.html

> like insurance1472.com and insurance060.com. He smelled a swindle, and he calculates it has cost his business more than $100,000 since 2003. M. F. is a victim of click fraud: a dizzying collection of scams and deceptions that inflate advertising bills for thousands of companies of all sizes. The spreading scourge poses the single biggest threat to the Internet's advertising gold mine and is the most nettlesome question facing Google and Yahoo, whose digital empires depend on all that gold. The growing ranks of businesspeople worried about click fraud typically have no complaint about versions of their ads that appear on actual Google or Yahoo Web pages, often next to search results. The trouble arises when the Internet giants boost their profits by recycling ads to millions of other sites, ranging from the familiar, such as cnn.com, to dummy Web addresses like insurance1472.com, which display lists of ads and little if anything else. When somebody clicks on these recycled ads, marketers such as MostChoice get billed, sometimes even if the clicks appear to come from Mongolia. Google or Yahoo then share the revenue with a daisy chain of Web site hosts and operators. A penny or so even trickles down to the lowly clickers. That means Google and Yahoo at times passively profit from click fraud and, in theory, have an incentive to tolerate it. So do smaller search engines and marketing networks that similarly recycle ads."[23]

4.4 Summary of offences from a technological perspective

From a technological perspective a cyberattack threatens all three of the main information security criteria: availability, integrity, and confidentiality (Figure 4.9).

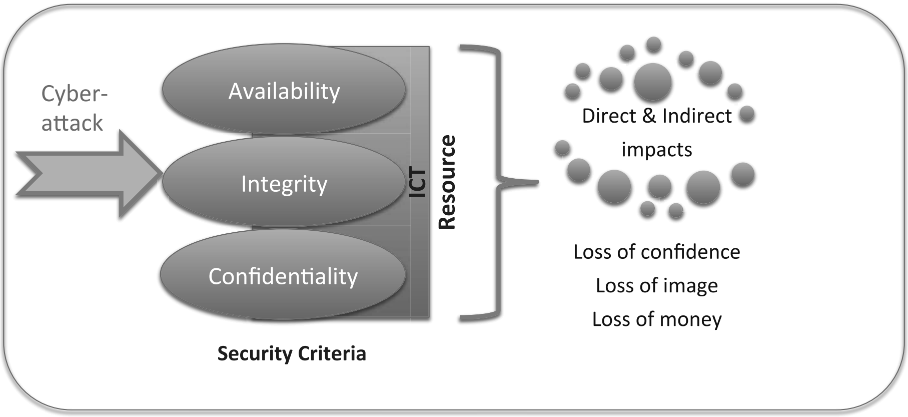


Figure 4.9 Main ICT security criteria.

[23] http://www.businessweek.com/magazine/content/06_40/b4003001.htm, 2 October 2006.

Availability

A resource's availability relates to its ability to be used to accomplish the service for which it has been designed. The availability rate of a network, a server or a file should be close to 100% during the service opening period, being available 24 hours a day, seven days a week, in order to provide the permanent capacity to meet users' requirements in an appropriate timeframe (the notion of accessibility and continuity of services). Some computing attacks consist of making some resources unavailable, damaging not only the users but also the owners of the resource.

Integrity

The notion of integrity expresses the fact that resources, be they transactions, processing, services or data, have not been degraded or destroyed. This criterion contributes to assuring the security of a piece of information in that it has not been accessed and that its contents have not been modified. Confidence can be placed in the correctness and reliability of this information because it can be demonstrated that it has not been modified or deleted without the owner's authorization.

Some malicious acts consist of modifying or falsifying information in order to have an impact on a particular decision (for example, the modification of an organized market leading to the sale or purchase of stocks). Acts of misinformation or cyberpropaganda do exist and are used to manipulate public opinion by providing false information, as could be the case of the modification of information on the website of a political party.

The integrity of hardware can also be affected by physical destruction, deterioration, or by deliberately provoked damage. Acts of sabotage that create obstacles to the legitimate use of systems can harm the integrity or the availability of the resources.

Confidentiality

Confidentiality is the fact of keeping information secret. As a security criterion, confidentiality is protecting data against unauthorized disclosure. Having data intercepted, monitoring individuals, and using IT to perform acts of espionage can have a negative impact upon:

- professional secrecy;

- fundamental rights, especially the right to intimacy and to a private life including digital intimacy, and the right to the respect of correspondence;
- the efficient functioning of organizations and the economy; and state security.

Security problems do not always have a criminal origin

It is important to underline that the attainment of these security criteria can also be affected by acts of non-criminal origin, such as the failure of electrical infrastructures. Moreover, a natural disaster or accident, such as an earthquake, a flood or a fire, can render a computing infrastructure unusable in exactly the same way as the incompetence of users, errors in design, or mistakes in using the systems. In respect of computer security, we should always keep in mind the principle born of long experience that while incidents or problems can have a criminal origin, it is more common for disasters to be linked to unintentional errors than to malevolence.

4.5 Case study from the FBI

A cyber-fraud scheme[24]

> *Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business. Malware Secretly Re-Routed More Than 4 Million Computers, Generating at Least $14 Million in Fraudulent Advertising Fees for the Defendants*
>
> According to the Indictment unsealed today in Manhattan federal court: Internet advertising is a multi-billion-dollar industry in which website owners sell advertising space on their sites. Because of the vast number of website operators – also referred to as publishers—and advertisers on the Internet, advertisers often rely on third party “ad brokers” to contract with and deliver their advertisements to publishers. Similarly, rather than contract with ad brokers individually, website publishers often join together and form “publisher networks” to contract with ad brokers collectively.

[24] U.S. Attorney’s Office, 9 November 2011 – Southern District of New York (212) 637-2600 http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

As alleged in the Indictment, from 2007 until October 2011, the defendants controlled and operated various companies that masqueraded as legitimate publisher networks (the "Publisher Networks") in the Internet advertising industry. The Publisher Networks entered into agreements with ad brokers under which they were paid based on the number of times that Internet users clicked on the links for certain websites or advertisements, or based on the number of times that certain advertisements were displayed on certain websites. Thus, the more traffic to the advertisers' websites and display ads, the more money the defendants earned under their agreements with the ad brokers. As alleged in the Indictment, the defendants fraudulently increased the traffic to the websites and advertisements that would earn them money. They accomplished this by making it appear to advertisers that the Internet traffic came from legitimate clicks and ad displays on the defendants' Publisher Networks when, in actuality, it had not.

To carry out the scheme, the defendants and their co-conspirators used what are known as "rogue" Domain Name System ("DNS") servers, and malware ("the Malware") that was designed to alter the DNS server settings on infected computers. Victims' computers became infected with the Malware when they visited certain websites or downloaded certain software to view videos online. The Malware altered the DNS server settings on victims' computers to route the infected computers to rogue DNS servers controlled and operated by the defendants and their co-conspirators. The re-routing took two forms that are described in detail below: "click hijacking" and "advertising replacement fraud." The Malware also prevented the infected computers from receiving anti-virus software updates or operating system updates that otherwise might have detected the Malware and stopped it. In addition, the infected computers were also left vulnerable to infections by other viruses.

Click Hijacking

When the user of an infected computer clicked on a search result link displayed through a search engine query, the Malware caused the computer to be re-routed to a different website. Instead of being brought to the website to which the user asked to go, the user was brought to a website designated by the defendants. Each "click" triggered payment to the defendants under their advertising agreements. This click hijacking occurred for clicks on unpaid links that appear in response to a user's query as well as clicks on "sponsored" links or advertisements that appear in response to a user's query – often at the top of, or to the right of, the search results – thus causing the search engines to lose money. Several examples of click hijacking illustrated in the Indictment include:

- When the user of an infected computer clicked on the domain name link for the official website of Apple-iTunes, the user was instead taken to a website for a business unaffiliated with Apple Inc. that purported to sell Apple software.
- When the user of an infected computer clicked on a domain name link for Netflix, the user was instead taken to a website for an unrelated business called "BudgetMatch."

- When the user of an infected computer clicked on the domain name link for the official government website of the Internal Revenue Service, the user was instead taken to the website for H&R Block, a major tax preparation business.

Advertising Replacement Fraud

Using the DNS Changer Malware and rogue DNS servers, the defendants also replaced legitimate advertisements on websites with substituted advertisements that triggered payments to the defendants. Several examples of the advertising replacement fraud illustrated in the Indictment include:

- When the user of an infected computer visited the home page of the Wall Street Journal, a featured advertisement for the American Express "Plum Card" had been fraudulently replaced with an ad for "Fashion Girl LA."
- When the user of an infected computer visited the Amazon.com website, a prominent advertisement for Windows Internet Explorer 8 had been fraudulently replaced with an ad for an email marketing business.
- When the user of an infected computer visited the ESPN website, a prominent advertisement for "Dr. Pepper Ten" had been fraudulently replaced with an ad for a timeshare business.

The defendants earned millions of dollars under their advertising agreements, not by legitimately displaying advertisements through their Publisher Networks, but rather by using the Malware to fraudulently drive Internet traffic to the websites and ads that would earn them more money. As a result, the defendants and their co-conspirators earned at least $14 million in ill-gotten gains through click hijacking and advertisement replacement fraud. The Indictment further alleges that the defendants laundered the proceeds of the scheme through numerous companies including, among others, Rove Digital, an Estonian corporation, and others listed in the Indictment.

The defendants' scheme also deprived legitimate website operators and advertisers of substantial monies and advertising revenue. In addition to search engines losing revenue as a result of click hijacking on their sponsored search result listings, advertisers lost money by paying for clicks that they believed came from interested computer users, but which were in fact fraudulently engineered by the defendants. Furthermore, the defendants' conduct risked reputational harm to businesses that paid to advertise on the Internet – but that had no knowledge or desire for computer users to be directed to their websites or advertisements through the fraudulent means used by the defendants.

Questions on the above case:

- Identify the principles on which the fraud is based and the types of means employed.
- What relationship is there between click hijacking and advertising replacement fraud?

4.6 Exercises

1. Why can the Internet present an element of performance efficiency for economic crime?
2. What problems are caused by the coming together of the worlds of organised crime and economic crime?
3. What is “ransomware”? What is the basis on which it works?
4. What are the key characteristics of the Internet that make it useful in money-laundering?
5. Describe a scenario in which a cyberattack damages the reputation of an organisation.
6. How can a cyberattack be viewed as a theft of resources?
7. Define what is meant by the theft of IT services and give an example.
8. What are the main consequences for a business when its data is stolen and its IT resources are taken hostage?
9. In what way does the Internet make software piracy easier?
10. From an IT perspective, how can cyberattacks be identified?

Chapter 5

Cybercrimes Against States

5.1 Understanding the context

Cybercrimes against public institutions and states can be classified in the following categories (Figure 5.1):

- manipulation of information and information warfare;
- intrusion into governmental systems and into computer systems controlling critical infrastructures;
- surveillance, espionage;
- disruption of e-government services;
- cyberwar;
- cyberterrorism.

Although the targets or end results of cyberattacks are different from those aimed at privately-owned businesses, the means of attack are identical, as are sometimes the identities of the perpetrators.

Everything that has been mentioned in the preceding chapters can also apply to criminality affecting states, be it directly or indirectly, through the IT resources of their ministries, governmental agencies, public services, or through their critical infrastructures.

The objective of this chapter is to illustrate by means of concrete examples how this kind of cybercriminality manifests itself, with Chapter 6 being dedicated to the specific topics of cyberwar and cyberconflicts, and of information wars, by and through information.

In March 2011 a hacking attack on the IT systems of RSA Security that was specifically targeted at their SecureID security product (a token used for two-factor authentication, widely used by organisations and businesses such as banks, the defense sector, and software houses) left these customers additionally exposed to cybercriminality.

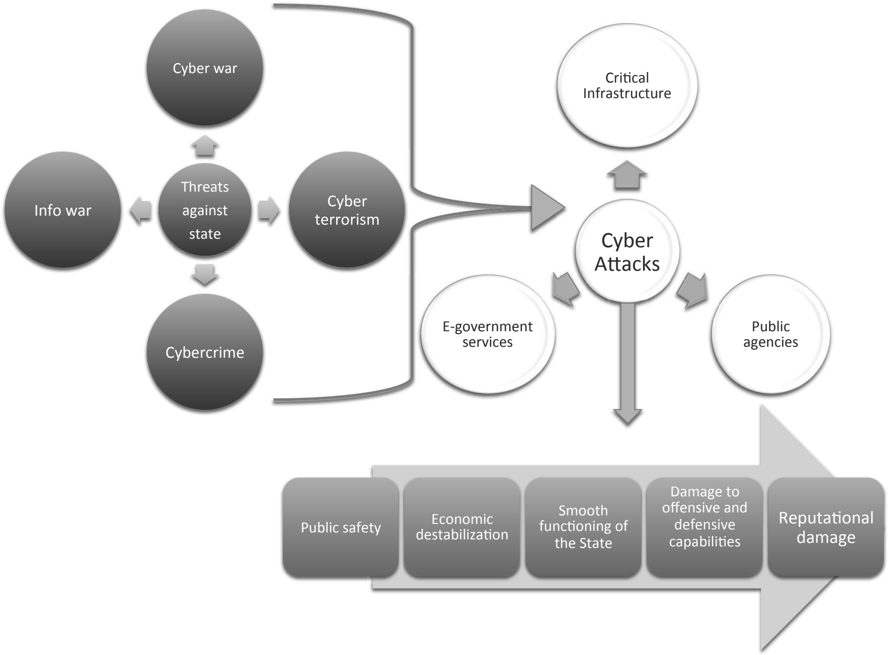


Figure 5.1 Crimes against public institutions and states.

From the press

> RSA Security has confirmed that stolen data about the company's *SecurID* authentication token was used in the recent attack against defence contractor Lockheed Martin. RSA has offered to replace the compromised tokens for high-risk customers. The RSA breach, reported March 17, 2011, was the result of what the company called an "extremely sophisticated" attack. The company said that it believed the likely motive was to take data that could be used against defence contractors rather than against financial institutions or to steal personal information […] RSA confirms its tokens used in Lockheed hack – RSA Security has confirmed that stolen data about the company's SecurID authentication token was used in the recent attack against defense contractor Lockheed Martin. RSA has offered to replace the compromised tokens for high-risk customers.[1]

[1] http://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx, Jun 07, 2011

For RSA Security – EMC, the financial losses arising from this attack are directly related to the replacement of the relevant security products. These losses are considerable, in the order of tens of millions of dollars ($66 million, according to one early report[2]). Even if these losses can be reasonably well quantified, however, this is not the case for the indirect losses caused by the damage to the company's reputation, to its image, to the customer confidence on which it depends, and for the subsequent losses incurred as a result of the losses suffered by those customers. Although RSA was able to publish the following statement, the confidence of its customers was irrevocably shaken, with the financial consequences that would be expected:

Whoever attacked RSA has certain information" about the product, "but not enough to complete a successful attack without obtaining additional information that is only held by our customers," the company said.[3]

In February 2012 the source code for several of the Symantec corporations security products (including pcAnywhere and Norton Antivirus) was published on the Net. This significantly increased the risk that users of these products could have their systems hacked. An unusual element about this case was that the hackers demanded a ransom of $50,000 from Symantec to not publish the material. But the negotiations failed between the hackers and the FBI agents to whom Symantec had reported the extortion, and thus the threat became reality.

These two examples of IT hacking show how companies providing security solutions can be targeted through the very solutions that they supply to public bodies or governmental agencies to protect their information systems.

5.2 Examples of cybercriminal activities that can affect states

The manipulation of information

The dissemination of information and disinformation is part of the political strategies of organizations and states. Manipulation can take many forms, for example the leaking of internal documents in order to destabilize a company or a state. The Internet lends itself to spreading rumours and disinformation in order to gain economic advantage or to manipulate public opinion.

[2] "In its earnings call Tuesday, EMC disclosed that it spent $66 million in its second quarter to deal with a cyber attack that compromised its RSA Security division." http://secureworldpost.secureworldexpo.com/?p=2565 – July 28, 2011

[3] http://gcn.com/articles/2011/03/23/rsa-securid-hack-update.aspx, March 23, 2011

The Internet can fund campaigns intended to spread disinformation or uncertainty. It also facilitates espionage and other intelligence-gathering activities, thanks to the vulnerabilities of ICTs and the ease with which information travelling across the Internet can be intercepted.

Today, national security faces challenges in the form of criminal threats related to information technologies. Internet technologies are at the heart of the notion of infowar or cyberwarfare, whose objectives are primarily economic; it can have a huge impact on the conduct of business operations.

Examples of damage to reputations and misinformation adapted from real cases

In 2005, governmental websites in a certain country were the targets of hackers. The hacked sites were all affiliated with the government, including those of the Department of Justice, the Department of Arts, Culture and Technology, the Films and Publications Board, the main Government Information portal, and the Government's open source website. The group of hackers, claiming to come from another specific country, first attacked the most important government server, from which it was easy to shut down all the websites hosted on it. The hackers left an insulting message. Once the websites were operational again, some were hacked a second time by a different group, who left the message "hacked by […] just for fun." The main areas of damage caused were in the slowing down of the development of public confidence in eGovernment services and in the possible negative impacts on the Government's reputation.

In 2005 and 2006, different groups of hackers defaced the homepage of the Public Service Commission of a country and left the following message: "How Can You Hire Somebody That Doesn't Know How 2 Setup a Public server? This Site Hacked by […]" In 2006, some hackers hacked a Defense Ministry Network and inserted a fake press release denouncing a big bribery scandal. Everything was planned to spread this lie on a large scale in order to damage the public image of the country's government. When internal security teams discovered the intrusion, it was already too late. Newspapers had already reported the scandal, affecting the image of the Ministry.[4]

The Wikileaks Affair, which broke in 2010, is not strictly speaking a case of cybercriminality, even if cyberattacks have subsequently been carried out

[4] These cases have been taken from www.zone-h.org and anonymized.; www.crime-research.org

by groups or individuals against the sites of institutions hostile to Wikileaks[5] in order to show their support for Wikileaks, and the Wikileaks site itself has been the target of cyberattacks.[6]

Regardless of the positive or negative opinion that anyone might hold about the information published through Wikileaks, opinions based on personal values and perspectives, the Wikileaks Affair is important as a point of focus for discussion of the idea of the freedom of expression on the Internet and of the limitations of traditional means of censorship and controlling the flow of information.

The Internet is at the same time a fantastic communications tool and an instrument of power for those who control it. "Mythology reminds us that every technological advance is a double-edged sword, not, as we might say prosaically, as a result of the good or evil use that we might make of it, but because of the changes it brings about to the split and exercise of power. It takes power away from some and gives it to others, thereby changing the world for everybody."[7]

This affair is the first of its size that allows us to recognise, once again, that the Internet is now part of the geostrategy of state and non-state actors in the context of the war for and through information, information to be used by isolated individuals or states, across the whole planet. At the same time, this technology has moved borders and upset the logic of transparency. Until now it has been the citizen or the consumer who has had to remain transparent, but since Wikileaks, it has also been a concern of states whose diplomatic secrets, for example, have been revealed. We have seen confidential documents belonging to diplomats, administrations, governments and armies made available to the general public on a global scale.

[5] "The loosely organized campaign to avenge WikiLeaks against those who have obstructed its operations, calling itself Operation Payback, has already temporarily brought down the websites of Visa and MasterCard, and of the Swedish government. A succession of U.S. institutions has withdrawn services from WikiLeaks after the website published thousands of sometimes embarrassing secret U.S. diplomatic reports that have caused strains between Washington and several allies." http://www.reuters.com/article/2010/12/09/us-wikileaks-idUSL3E6N80HH20101209, 9 December 2010.

[6] "Cyber attack forces Wikileaks to change web address" http://www.bbc.co.uk/news/world-us-canada-11907641; 3 December, 2010.
"WikiLeaks site comes under cyber attack – WikiLeaks website crashes in what appeared to be a cyber attack following the publication of state department cables"
http://www.guardian.co.uk/world/2011/aug/31/wikileaks-site-cyberattack-cable-release
Associated Press – guardian.co.uk, Wednesday 31 August, 2011

[7] R. Berger, S. Ghernaouti-Hélie, "Technocivilisation, pour une philosophie du numérique." Focus Sciences PPUR 2010.

What is doubtless new in this affair is that for once it is not the humble citizen who is being stripped bare: usually it is the individual who is forced to submit to the monitoring of surveillance cameras or security equipment at airports, or is encouraged to reveal all on social networks; it is the individual who is traceable through communications and electronic transactions (mobile telephones, payment cards, transport tickets). On the Internet, everything can be learned about other users. In addition, the ability to supply very personal information is provided to everyone and affects everyone. Perhaps now the message has been passed to those in charge that they cannot allow themselves to say or do whatever they like – in case the details are published on the Internet.

How can personal information and secrets be protected? How can we be protected from their publication by third parties who have acquired them, be it through legal or illegal means? How can these needs be reflected in effective cybersecurity measures? This is a matter that concerns individuals, organisations and states, and the answers to these questions are complex.

Hacking governmental websites

The websites of national bodies, local governments, research institutes, educational institutions, or government affiliates can be targeted and defaced. Hacking into governmental websites is a form of information warfare. The motivation for such crimes can vary from political expression to service disruption, passing through damage to reputations, loss of trust and confidence, destabilization, and information warfare. In this context, hacking computer systems is a form of political activism ("hacktivism")[8], resistance or protest, as shown by the following examples.

Examples – Cases of loss of trust and confidence in governmental institutions[9]

In 2004, a group of hackers attacked an official country website designed to show the progress of an ongoing vote count. The attackers changed the names of political parties into fake names, such as "Pink Grandfather Party," "the Party of Bottled Mineral Water." Investigation showed that more than thirteen

[8] See also Chapter 6.

[9] Theses cases have been inspired by information found on the following websites: www.news.zdnet.co.uk; www.crime-research.org

other political groups' names have been attacked. In 2003, hackers defaced the website of a country Police Department and made it into a pornographic site with obscene pictures on the first page. "The links – and the pop-up screens – connect to websites where more pictures and invitations to 'live shows' are waiting."

Examples – Cases of service disruption[10]

In 2005, a group of hackers attacked a country's Defence Ministry website. This website was designed to provide scholarships for military personnel. The Internet homepage was attacked twice within a few weeks, and this lead to a temporary shutdown. Possible damage caused included the theft of the stored personal information of military personnel, such as bank account numbers, registration numbers, and addresses.

In 2000, hackers attacked a country's telecommunication regulatory agency website. Investigation showed that the attack was launched from two countries. The hackers launched a denial of service attack leading to the outage of the website; the site received 600 hits per second in the first 90 minutes of the attack. The main damage was the downtime of the site, which lasted around 6 hours.

In 2003, a satellite television network was the target of distributed denial of service attack. A large amount of traffic was sent to the name servers responsible for the targeted websites, leading to the breaking down of services. This attack aimed to disrupt television network servers and thus to shut down all related services. The main negative consequence was the decision of hosting companies to stop hosting the site in order to maintain service to their other customers.

Most often service disruption is performed through denial of service attacks, as it is the case in the following example from 2011.

> The Serious Organised Crime Agency (Soca), the UK national law enforcement unit dubbed the "British FBI," has been forced to take its website offline after it was targeted with a distributed denial of service (DDoS) attack. [...] It is thought to be the first time a British law enforcement website has been crippled by the group LulzSec, which has previously attacked sites belonging to the US Senate, the

[10] These case have been anonymized from various sources as: www.zone-h.org; www.news.zdnet.co.uk; www.crime-research.org; www.asiamedia.ucla.edu; www.newsbits.net; www.infoworld.com

> CIA, as well as the games firms Nintendo and Sony. […] A spokesman for Soca, the government agency that draws on expertise from the police, immigration and revenue and customs to investigate organised crime including drugs and people trafficking, said its website was taken offline to “limit the impact” of the attack. He added: “The Soca website is a source of information for the general public which is hosted by an external provider. It is not linked to our operational material or the data we hold.”[11]

Examples – Cases of political expression from the past[12]

In July 2006, some people hacked a government website of a country and left the following sentences: “www.C0RRUPT.com […] Defaced by […] “It looks like this country needs some help securing their shit while they are killing their whole goddamned country! Register on our forums and we’ll help you upgrade and secure your database […]”

In 2001, a hacker attacked two local government websites and defaced their homepages with obscene pictures. He substituted the name of a local representative by a discourteous name and the name of a major by “Idiot.” He also changed the title of the greeting message into “We are a Bunch of Hogs.” Given that the hacker also attacked commercial entities such as stock-exchange network, the damages were significant.

In 2002, a hacking group defending some militants attacked the official website of the Telecom Regulatory Authority of a country. They left the following message “regulatory authority has been defaced by […] for the freedom of […]”

In 2006, a specific hacking group attacked the website of a Country National Institute and defaced the website by substituting the historic research documentation of the country’s genocide by another country’s propaganda.

In 2001, some national websites, including a specific country’s Education Ministry and Political Party, were the target of hackers for online protest. The latter launched a denial of service attack using email bombs. Hackers, who were mostly students in a foreign country, attacked these websites because of a new history textbook glossing over atrocities committed during World War II and the occupation of specific countries. The website of the publishing company responsible for this textbook was also attacked.

[11] http://www.guardian.co.uk/technology/2011/jun/21/soca-website-hacking-lulzsec

[12] These case have been anonymized from various sources as:
www.zone-h.org; www.blonnet.com; www.infowar-monitor.net; www.niser.org.my

Examples – Old cases of destabilization and information warfare[13]

In 2006, a hacking group called "un-root" launched massive vandalism attacks on the governmental websites of a country, including the Health Ministry, the Council of Ministry, and the Ministry of Parliament Relations. In total, they hacked twenty-five official websites.

In 1998, the most sensitive nuclear weapons research facility of a country's Atomic Research Centre was the target of hacking attacks. Hackers claimed to have broken into their servers, stealing five megabytes of information and erasing nuclear data on two of six servers at one particular facility. Hackers left a message on the defaced website saying "Don't think destruction is cool, […]"

In 2004, a group of hackers based in a country launched a large attack on another country. The hackers used two information-stealing viruses (a variation of a Trojan hacking program and a specific Backdoor). The hackers broke into 211 computers of ten government agencies, such as the National Assembly, the Maritime Police Agency, the Agency for Defence Development, the Atomic Energy Research Institute, the Institute for Defence Analysis, the Air Force Academy, the Small and Medium Business Administration, and the Astronomy Observatory. These targets are sensitive state organizations; the Agency for Defence Development is involved in weapons development. The hackers also targeted 67 computers from private companies, universities, and media firms. Investigation showed that information on 122 people was stolen in the attack on the National Assembly.

In 2005, a particular hacking group hacked a country government website registered and left the message: "You abuse […] (people) in your country, while I abuse (hack) your web-pages, and it won't stop until you stop. […] Don't forget that we watch what happens with […] (people) in your country. Don't forget that we watch and ATTACK […]"

In 2006, after a military bombardment, many different groups of hackers attacked websites of the aggressor state by launching bombing attacks, intruding on websites and defacing web pages. Some defacements were carried out to stop the military attacks, such as the plea, which focuses on the condition of families by saying "... don't shut up to this oppression..!! When someone makes a movement it's a blame but they make it WHY everybody is silent…" A group of hackers defaced more than 700 websites registered under the domain of the aggressor state including banks, hospital and companies, with the same following message: "Hacked By […] u Kill people we Kill servers."

[13] These case have been anonymized from various sources as:
www.zone-h.org; www.news.zdnet.com; www.sophos.com; www.mima.gov.my

The following message was posted in 2005 on a Public Works Department website: “With respect, In the name of the law, I order you, government *x*, please retreat from area *y*. Please don’t be too greedy *y* is having bad days recently. The natural disasters, increasing poverty, etc. Your country is much more prosperous than *y*. Don’t you be ashamed? FYI: I’m not a hacker.”

As the above examples indicate, governmental websites (although not exclusively) have been the targets of attacks, of vandalism, of intrusions, and of the modification of data for many years. More recent examples can also be given, such as the one below. Nowadays such stories are reported by the press on a daily basis, to the point that they are becoming so common and banal that they no longer attract the attention of the media. This shows that the phenomenon of cybercriminality is very much a current issue and that the measures in place to combat it are insufficient and ineffective. It is important to note that attacks on institutional sites are growing in number and that responsibility for these attacks are increasingly, although not solely, being claimed, by people claiming to belong to groups such as Anonymous.

Example from the press

> *Hacking Ukraine: Govt retreats after massive cyber-siege*
>
> Ukrainian government websites have suffered a two-day cyber attack after the authorities closed a popular file-sharing service. The police have withdrawn the blocking order, but their investigation into alleged piracy is very much ongoing.
>
> Users lost access to dozens of official websites in Ukraine after they came under attack on Tuesday. Websites belonging to the president, the government, Ukraine’s security service, the national bank, and the interior ministry were among those affected.
>
> The cyber offensive was fuelled by thousands of internet users trying to protect the popular file-sharing service, EX.ua. The site, which is similar in function to Megaupload.com, was closed by the authorities on Tuesday.
>
> Ukrainian police allege that the site was involved in online piracy. The interior ministry searched EX.ua offices and seized some 200 servers containing more than 6,000 terabytes of data.
>
> The move triggered an instant tsunami of anger among Ukrainian internet users which quickly spilled over in a series of hacker attacks on the government. According to sources in the movement, the virtual siege involved about 500 IT professionals and hundreds of thousands of ordinary users who flooded the websites with requests in a bid to force them offline.
>
> The attackers were prepared to seek help from the hacktivist group Anonymous, reports the news website Ukrainian Pravda, citing a letter received from one of the hackers involved in the situation.”[14]

[14] http://rt.com/news/ukraine-hacker-attack-triumphant-411/; 03 February, 2012.

5.3 Cyberthreats against states

About cyberattacks on critical infrastructures and terrorism

National security, public safety, and the effective functioning of the economy rely on infrastructures that are considered essential for states, organizations, and individuals. Communications, electricity or water distribution infrastructures, and the infrastructures for financial or health institutions, for example, can be considered as critical. The nature of critical infrastructures and the degree of importance vary from one country to another. Critical infrastructures are currently controlled or accessed via information and communication infrastructures, which mostly belong to private or foreign actors and are administrated by the private sector (producers and distributors of electricity, telecommunications operators, etc.). Opponents of states or organizations can attack systems or infrastructures in order to use them, destroy them, or find material for blackmail. Vulnerabilities in information and communication technologies can be exploited in pursuit of political goals.

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.[15]

Example

In 1999, during some presidential elections, some hackers defaced about 165 websites, in order to affect the country's infrastructure, including electricity, economic institutions, telecommunications, and air-traffic control.[16]

The vulnerability of the essential infrastructures of a country (energy, water, transportation, food logistics, telecommunication, banking and finance, medical services, government functions, etc.) is increased as the use of Internet technologies takes root.

Particular emphasis needs to be placed on the systems for the generation and distribution of electrical power, which are essential to the operation of most infrastructures. One of the key objectives of cyberopposition appears to be the control of critical elements of infrastructure, as shown by the increase in

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

[16] www.niser.org.my

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.

From the press

> An Italian researcher has uncovered at least a dozen security flaws in software used in utilities and other critical infrastructure systems, prompting security advisories from the U.S. government. Security researcher L. A. disclosed the attacks against six SCADA (Supervisory Control and Data Acquisition) systems including U.S. giant Rockwell Automation. The step-by-step exploits allowed attackers to execute full remote compromises and denial of service attacks. Some of the affected SCADA systems were used in power, water and waste distribution and agriculture. Such zero-day information disclosure was generally frowned upon in the information security industry because it exposed customers to attack while published vulnerabilities remained unpatched. Attacks against SCADA systems were particularly controversial because exploits could affect a host of machinery from lift control mechanisms to power plants.[17]

The term "cyberterrorism," or terrorism applied to cyberspace, which has come into vogue recently, should be used with care; there is no clear agreed-upon definition of what constitutes cyberterrorism. It might be better to use the generic term of cyberthreats. Terrorism is generally understood as the systematic use of violence to achieve political aims. The question is posed whether the breakdown of the Internet, or a portion of it, and the carrying out of various cybercrimes as a result of malicious acts, might not sow terror within a particular community of users. Apart from symbolic threats to the Cyberworld, cybercrimes against critical infrastructures can endanger human life by creating an indirect menace to people. In this context, cybercrime can have a terrorist dimension.

Most often, the term cyberterrorism covers a fairly vague catalogue of cyberthreats. 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 try to extrapolate the thinking that might have motivated a hacker, mercenary, activist, ordinary criminal, or prankster, and thus try to determine what the criminal intention was behind the acts. The type of computer-related attack cannot be used to state the motivation or aims of the attackers with any certainty.

[17] http://thehackernews.com/2011/09/0-day-scada-exploits-publicly-exposed.html

Whether it is through a process of economic destabilization by threatening critical infrastructures, spreading ideology, or manipulating information, cyberthreats constitute a new set of strategic threats that must be taken very seriously by states (Figure 5.2).

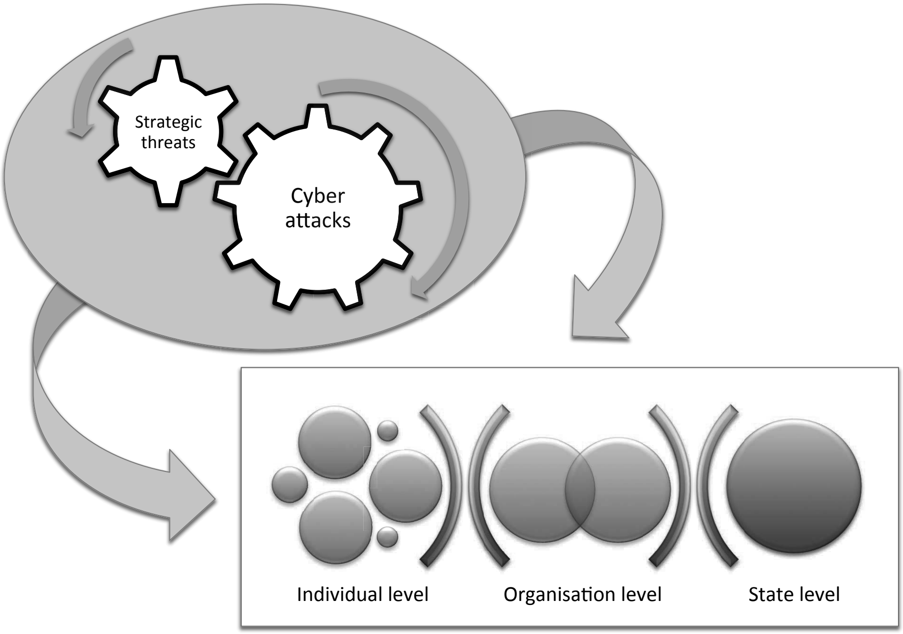


Figure 5.2 Cyber threats against states and critical infrastructures.

Examples of hostile cyberactions

At the moment opponents can use information and communication technologies (ICT) to perform hostile actions for political objectives. Some opponents of states or organizations use the Internet as a means of proselytizing and recruiting new adherents (websites can contain photos, interviews and video of training, for example). The following examples show that ICT has been used all over the world, and for a long time, to contribute to activism, to recruit, to train, to finance, or to gather information to perform attacks outside cyberspace. Main players used the Internet to disseminate information, to conduct propaganda, to recruit adherents, and also to cause damage. Hackers used Internet networks to condemn aggressions, by breaching government computers and disrupting services. The Internet is nowadays a means of communication for reaching a large audience and spreading worldwide propaganda.

Example – Case of retaliation

> "The take-down of Megaupload.com, one of the world's biggest filesharing websites, has prompted swift retaliation from self-styled "hacktivist" group Anonymous, which has launched a string of online attacks against US government bodies including the FBI and the Justice Department. Anonymous, an online hacker collective, said it had launched its largest attack ever in retaliation for the closure of Megaupload. Megaupload was taken offline on Thursday January 19, 2012 after US prosecutors accused seven men behind the site of cheating copyright holders out of $500m (£323m) in revenue over five years… hackers associated with Anonymous managed to briefly disable several US websites including those for the White House, FBI, Department of Justice and others associated with Warner Music and Universal Music […]"[18]

Examples – Cases of activism and propaganda[19]

In 2004, cybercriminals hacked a server operated by a country's highway office in order to distribute 70 files containing video featuring Mr. Nobody. For several years they have been taking advantage of the Internet for recruiting, organizing, and training.

A country used the Internet for carrying out a propaganda campaign. It administered three websites designed to be a central press office, to describe attacks targeting another country and to spread news and information.

In 1998, the website of a country's Information Centre was the target of hackers who claimed to be members of the a terrorist organization. They defaced the website by posting another country's national symbol and the following message: "Welcome to the Web page of the biggest liars and killers!," and "Brother, this coat of arms will be in your flag as long as you exist!" The website was restored in few hours but the hackers hit again and left a message saying, "This site is hacked by […] Hackers Team […] Long Live Great […]!!!"

[18] The Guardian "Anonymous launches attacks in wake of Megaupload closure"
Josh Halliday, Friday 20 January 2012
http://www.guardian.co.uk/technology/2012/jan/20/anonymous-attacks-after-megauploads-closure

[19] These cases have been anonymized from various sources as:
www.crimeresearch.org; www.news.com; www.anzen.mofa.go.jp; www.news.bbc.co.uk

Examples – Cases of the disruption of service[20]

In 2000, hackers attacked a specific website in order to encourage supporters to launch an attack by flooding the site with emails. The attacked website retaliated by taking down an important government website, and the Foreign Ministry website. This game of "replay attacks" continued for some months through website defacements and denial of service attacks. During the same year, hackers attacked Internet service providers, leading to a disruption of services and e-commerce sites. The main consequence was an eight percent dip in the country's stock exchange.

From Interpol

> The global nature of the Internet has allowed criminals to commit almost any illegal activity anywhere in the world, making it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace. The use of the Internet by terrorists, particularly for recruitment and the incitement of radicalization, poses a serious threat to national and international security.
>
> In addition, the threat of terrorism forces authorities to address security vulnerabilities related to information technology infrastructure such as power plants, electrical grids, information systems and the computer systems of government and major companies.[21]

At the same time, when financial markets or stock exchanges are affected by IT attacks, it is not only the business sector that is impacted, but perhaps also the whole country. It can be noted that international organisations are not spared from cyberattacks. These attacks can continue for several years before being detected and halted, as the media report in the example below.

From the International Business Times

> Hackers stole data from more than 70 international organizations and businesses in a sweeping five year cyber attack that could offer fresh evidence of a broad Chinese hacking offensive.
>
> Hackers infiltrated organizations that ranged from international entities like the United Nations and the International Olympic Committee to U.S. defense firms

[20] Adapted and anonymized from www.d-n-i.net/ ; www.niser.org.my

[21] http://www.interpol.org/Public/Children/SexualAbuse/NationalLaws/Default.asp

to the Associated Press, according to an analysis conducted by the security firm McAfee. 49 of the 72 cyberattack targets were in the U.S.[22]

New cyber threats

It is impossible to draw up an exhaustive list of all the possible impacts on the security of a state or its citizens. The omnipresence of IT equipment and its use in all areas of human activity mean that the risks of erroneous use, hijacking, or criminal manipulation are permanent and can have an effect on civilians and military personnel, on every structure and on every individual.

The new threats that have evolved can also affect GPS guidance systems, be they used for civilian or military applications. The consequences of such attacks could be impressive when they involve, for example, the use of weapons guided at a distance by GPS (drones, missiles), and could be equally dramatic when directed at applications used for logistics or supply chain management.

Human activity is above all a story of movements. The control and management of the movements and behaviours of individuals, combined with the circulation of objects and animals implanted with technologies that allow geolocalisation (RFID chips, smartphones, GPSes, Tablet PCs, laptops, Internet devices), have become high-stakes issues for society. With geostrategic, economic and societal impacts, the technologies used for geolocalisation and the various uses that are made of the data they yield are forcing us to re-examine the concept of the protection of data and systems, and to consider the most effective means of securing them.

5.4 Summary

As the preceding examples have shown, cybercriminality can act in various ways in opposition to states, with degrees of intensity and consequences of greater or lesser significance, ranging from simple nuisance to political and economic destabilisation, and even to death. This could result, for example, from cyberattacks launched against information systems used to control production at a chemical plant, a water treatment facility, or a pharmaceutical

[22] http://www.ibtimes.com/articles/191690/20110803/cyber-attack-china-cyber-warfare-china-massive-cyber-attack-china-hacking-mcafee-hacking.htm, August 3, 2011

factory, or against control systems used for aerial traffic, railways, or hospital equipment (operating theatres, breathing apparatus, etc.).

5.5 Exercises

1. Are there any differences between cybercriminal attacks on the information systems belonging to private organisations and those attacking state systems? If so, how can these differences be identified?
2. What could be the objectives of cybercriminal acts aimed at states?
3. Give an example of the breakdown of a system used in e-administration following a cyberattack, and identify the potential consequences.
4. Give examples of cyberattacks that contribute to destabilising a state and identify in what way the general public could be affected.
5. Suggest a catastrophe scenario for public security that is the result of one or several cyberattacks.
6. What are the risks for a state related to cyberattacks aimed at supply chain management?
7. Identify the main ways in which states are dependent on telecommunications infrastructures and the new threats that they carry.
8. In what way is cybervandalism becoming a weapon for states?
9. How can a state be sure of the identity and motivations of its cyberattackers?
10. Why is the control of geolocalisation systems (such as GPS) important for individual states?
11. Provide examples of the hijacking, abuse, or hacking of services using geolocalisation data that have an impact on:
    (a) individuals;
    (b) organisations;
    (c) states.

Chapter 6

Cyberconflicts, Cyberwars and Cyberpower

6.1 Understanding the context

Cyberattack: a question of terminology and meanings

The term "cyberattack" can have several meanings, depending on the targets, victims, motivations of the perpetrators, scope, impact, and the consequences of the attacks. Some have minor impacts and can often be attributed to straightforward delinquency, while others could have drastically negative effects on people, organizations, and states, and could be linked to crime, terrorism, or war.

When combining the impact on a specific target with the generic consequences of an attack in the wider world, it is possible to develop a classification of cyberattacks having significant negative impacts on society. Such a classification could take the form of:

- attacks on public safety through the manipulation of the ICT systems involved in the management or control of vital infrastructures (flight, railway or subway control systems, water or flood supply control systems, health control systems, financial and banking control systems, electricity grid control systems, Supervisory Control and Data Acquisition (SCADA systems). This category also includes all types of attacks on the ICT systems and infrastructures used in disaster recovery plans;
- attacks on national defense systems involved in offensive or defensive military activities;

- attacks on e-government systems;
- attacks that lead to the manipulation of information (cyberpropaganda), to intelligence gathering, and to electronic espionage;
- attacks involved in economic crime;
- attacks involved in the harassment of people;
- attacks combining elements of two or more of the above.

Because of the multiple interdependencies of ICT infrastructures, it is essential not to limit the analysis to one single perspective when considering the impacts of cyberattacks (Figure 6.1). These attacks could have several separate or domino effects, and human life could be endangered even if the cyberattack is not innately designed to do so. It is always difficult to identify such dependencies precisely in order to be able to control potential collateral damage, to understand the long-term effects, or to prevent the dramatic socio-economic effects of cyberattacks.

Very often the use of the word “cyberattack” instead of “cybercrime” indicates that the attacks were mostly directed against the computer and telecommunication systems involved in vital infrastructures that have a serious role to play in the economy, the safety of people, the sovereignty of a state, and the military and defence systems of a country. These attacks are offensive actions that alter, disrupt, manipulate, degrade, or destroy data, information and communication infrastructures (hardware or software). They could impact the

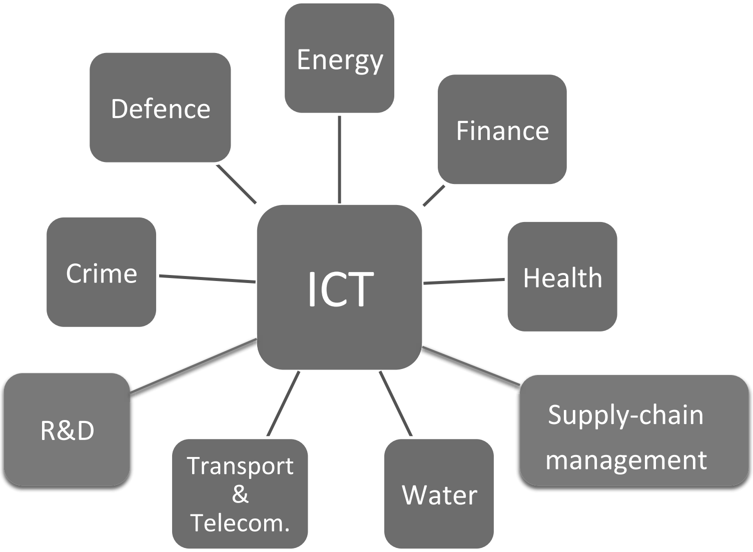


Figure 6.1 Interdependencies of ICT infrastructures.

whole of society by destabilizing, for example, the efficient operation of the economy or of governmental services.

In other circumstances, when a cyberattack leads to specific offences, it is most commonly described as a cybercrime. Such activities are typically characterized by, for example:

- offences against the confidentiality, integrity, and availability of information and communication resources, including illegal access to computers (by computer hacking or wiretapping, or by deceiving internet users by spoofing, phishing or password fishing), computer espionage, computer sabotage theft, destruction of data, intelligence gathering, etc.;
- offences against people, such as the computer-related online grooming of children, searching for potential victims, human trafficking, etc.;
- computer-related economic traditional crimes, such as frauds, manipulations, abuse of credit cards, forgery, swindles, extortions, money laundering, etc.;
- content-related offences, such as 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, etc.;
- offences related to the infringement of copyright and related rights, such as the unauthorized production and use of software, data, audio, and video, etc.;
- offences related to espionage.

For an attack to be identified and treated as a crime action that breaks a law, that law by definition must already exist. But cyberattacks exist without any laws to qualify them. The term cyberattack covers a broad range of activities and is independent of any specific classification of offenses. Terms and definitions are not yet well defined or broadly accepted, but it seems that an agreement has been reached for presenting cyber attacks by describing their modus operandi (the way a cyberattack is performed and its vectors of propagation), the consequence and impact on relevant security criteria, and their generic and global impact.

At the same time, the word *cyberattack* can also be understood as referring to a military weapon. ICT infrastructures, information/disinformation procedures, and cyberattack-related tools are increasingly being linked to war-making capacities that contribute to developing the potential for cyberwarfare.

Cyberconflict is a generic term that defines cyberattacks resulting from retaliatory actions between nation-states or organised groups as a response to contentious or conflict situations. When states themselves carry out cyberattacks within a military context, the term *cyberwar* is preferred (Figure 6.2).

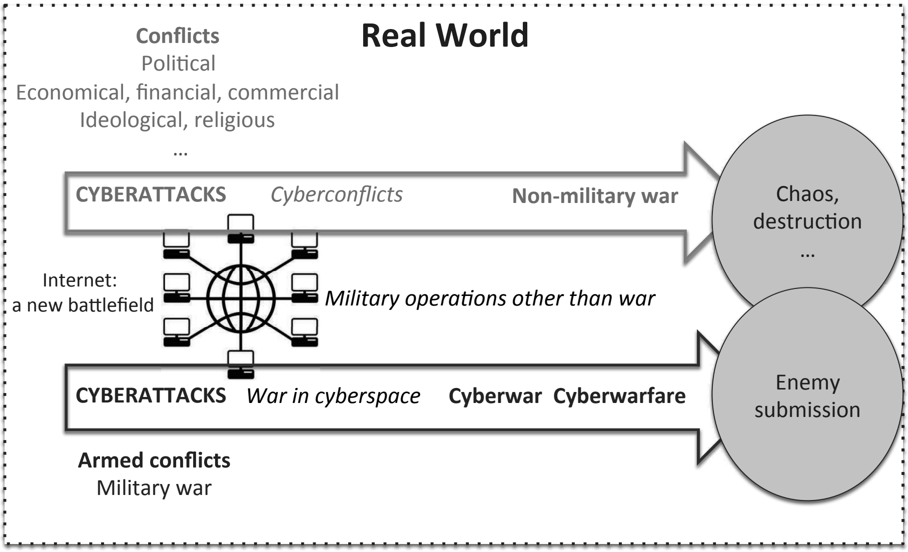


Figure 6.2 The notion of cyberconflict.

Nevertheless the term *cyberwar* should be used with caution, and only when cyberattacks are related to military personnel who are targeting systems operated by enemies and located in foreign countries. At present an amalgam of terms and concepts is in common usage, a situation largely supported by the media and by cybersecurity product and service providers; this has led to confusion and contributed to the development of fear of a phenomenon that is fluid and difficult to qualify. At the time of writing there have been no real cyberattacks of a purely military nature in the classical sense of the term, and thus it is surely preferable to refer to cyberattacks linked to cyberwarfare rather than cyberwar.

New battlefields and paradigms of war

It is true, however, that cyberspace has progressively become a political and a economical battlefield; cyberweapons (malware, hacking, DDoS, etc.) can potentially target, entirely indiscriminately, civilian ICT resources as well as cyber-based military systems. To some extent the Internet could be seen as a weapon of mass destruction, insofar as a program that could serve as an enemy, a spy, or a thief could be installed in any piece of electronic equipment. This is particularly true when considering, for example, the capabilities of malware for propagation and infection, the number of existing botnets and zombie servers that could be involved in a distributed denial of service attack, or the way that a country, a region, or even a continent can be cut off from the Internet.

Because of the multiple dependences and interdependencies between critical infrastructures, it is sometimes difficult to make the distinction between military and civil domains. Some cybersystems can belong to military bodies but be accessible through infrastructures useful for supporting the needs of the civilian sector. This is particularly true, for example, when considering systems for the production and distribution of electricity. In the same way, many vital infrastructures and services are dual-use or have primarily been built to support the needs of the civilian sector. Moreover, civilian ICT infrastructures can be important to the military sector to one degree or another and targeted by potential cyber attacks. If so, it could be difficult to qualify such a cyberattack as an act of war on the basis of its impact, as very often the source of the attack is not clear and the attack can be performed from multiple sources or by passing through several systems, networks, or countries. International cyberattacks can be performed though proxy systems and infrastructures, which makes the origin, the initiator, and the organizer difficult to determine, and makes it equally difficult to demonstrate that a particular government or agency was behind it.

New kinds of threats have emerged in cyberspace that affect and implicate both the civilian and military domains. Facing up to cyberattacks, whatever their aims and motivations, requires rethinking security and adapting military doctrine and defensive mechanisms (Figure 6.3). Identifying and understanding these new cyberthreats are important in developing effective cybersecurity measures and military cybercommand capabilities. The more developed a state is, the more its military capacities and economic power are dependent on information and communication technologies. They are then weakened because they are more vulnerable to major computing attacks.

Problems are created at multiple levels of society by security incidents related to natural catastrophes, errors, and failures, as well as ICT damages caused by human behaviour or misuses (including crime and terrorist acts), and the intensification and the increasing complexity and efficiency of cyber attacks.

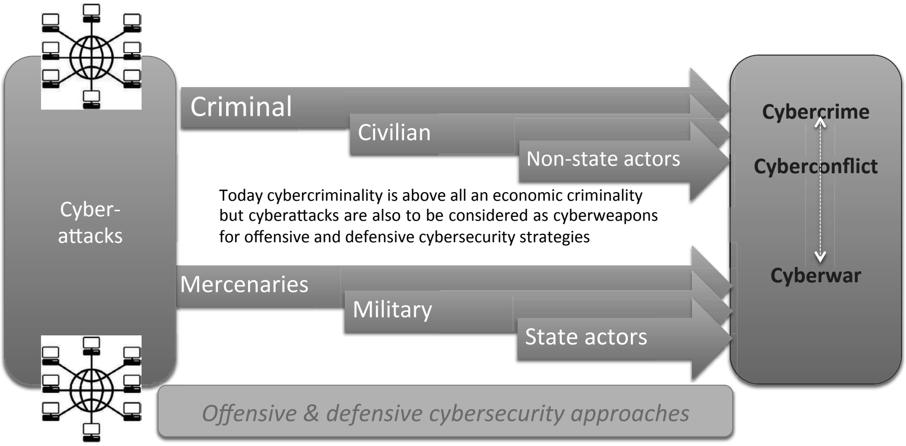

Cyber-attacks
Criminal
Civilian
Non-state actors
Today cybercriminality is above all an economic criminality but cyberattacks are also to be considered as cyberweapons for offensive and defensive cybersecurity strategies
Mercenaries
Military
State actors
Cybercrime
Cyberconflict
Cyberwar
Offensive & defensive cybersecurity approaches

Figure 6.3 New paradigms for crime, conflict, terrorism and war.

Not every cybercriminal action corresponds to terrorism or war between states. However, the Internet introduces new risks for states because it can become a weapon. The Internet can support a political project and be used in a situation of conflict, or even to harm an enemy without fighting, by reducing the enemy's power in economic, scientific, or cultural domains. No country is shielded against cyberactions aiming to harm it.

In a net-centric world, the Internet allows the use of indirect strategies that even in peaceful times can contribute to weakening a business sector, an enterprise, or a country, and thus generate competitive advantages to some socio-politico-economical players. The high stakes in play over controlling space, communications satellites, and GPS technologies are additional examples that illustrate the intense competition between states in the field of information technologies. Cyberspace is an ICT environment that countries have to master to ensure the smooth functioning of the state, even in peacetime.

Except for World War II, which was to a large extent ideological, wars have usually been executed for economic reasons, even if the justifications are presented differently. Even if, at our latitudes, the prospects of armed conflict have largely disappeared, due to the European Community and various alliances, the germs of economic war are always there, and these have moved onto the domain of information. Managing the Internet has thus become a strategic matter. Cyberspace, which until now has essentially served the civil society, is now being exploited by the military world that is using civil means as part of its operations. Terms such as *cyberattacks*, *cyberforces*, *cyber-offensives* and *cyberarmy* are now part of a vocabulary that is continuously developing and being enriched, thanks to the existing military nomenclature. It is not the evolution of the terminology that matters, but what it reflects: a reappropriation of the Internet by the military. Nowadays we know that cyberspace is not being used exclusively for peaceful purposes, but also for crime, terrorism and military activities.

6.2 From cybercrime to cyberwar

A common denominator

Usually crime-related issues and military issues are handled and studied separately by specialists in civil or military matters. Crime is a legal problem related to law enforcement and systems of justice and police. War has traditionally been a subject for military staff and specific governmental agencies. Nowadays, however, as we have seen, cybercrime and cyberwarfare are carried out using the same kind of tools, know-how and technical infrastructures. Cyberwarfare uses the same toolkits (malicious software, technical exploits) as those developed, used and made available by cybercriminals in underground markets. Because cyber-mercenaries exist in the marketplace and perform whatever is lucrative for them as a job, non-state actors can be involved in both cybercrime and cyberwar. The evolution of cyberattacks over the last decade is evidence of the abolition of frontiers between cybercrime and cyberwar (Figure 6.4).

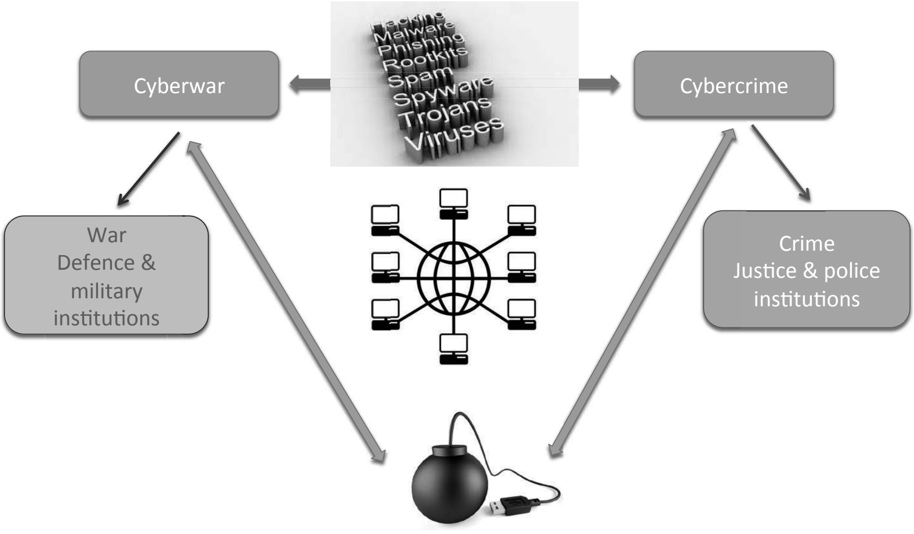


Figure 6.4 Cyberattacks: a common denominator.

To cite only one example, the Conflicker Worm, since its discovery in 2008, has infected government sites, military networks, and home computers all around the world. Several releases exist that have facilitated the propagation and infiltration of this worm.

Some examples of cyberactions aiming to damage states

Depending on the context, the actors, the political situation, and the geostrategic stakes, this type of cyber action can be largely mediated.

From the media

> *Estonia 2007*
> Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare. Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement. Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin. […] The Estonian government says its state and commercial websites – including a number of banks – are being bombarded by mass requests for information – overwhelming their computer servers. Targets of the so-called denial-of-service attacks have also included the Estonian foreign and defence ministries and leading newspapers and banks.
> In some cases, officials have simply blocked access to the servers from outside Estonia, to prevent them from being attacked. […] The defence ministry says that the cyber attacks come from all over the world, but some have been hosted by Russian state servers. It says that instructions on how to carry out cyber warfare are circulating in Russian on Russian websites.[1]
>
> *Russia – Georgia 2008*
> Caucasus foes fight cyber war – Armed with computers, unseen ranks of hackers are fanning conflict in the Caucasus. Internet users in Russia and Georgia have attacked vital websites in each other's countries, in a virtual echo of battles being fought on the ground by troops and tanks. Several Georgian government portals have been defaced or forced offline by hackers allegedly based in Russia. Visitors to Georgian President Mikhail Saakashvili's website were recently routed to a page portraying him as a modern-day Hitler. Georgia's parliament and foreign ministry sites have also repeatedly been disabled, allegedly by attacks from networks of hijacked computers.

[1] http://news.bbc.co.uk/2/hi/europe/6665145.stm, May 17, 2007.

Hackers from Georgia have meanwhile been blamed for targeting the websites of Russian news outlets and the separatist government of South Ossetia, which Russia supports.[2]

Stuxnet – Iran 2010
The Stuxnet outbreak – *A worm in the centrifuge* – A new software "worm" called Stuxnet (its name is derived from keywords buried in the code) seems to have been developed to attack a specific nuclear facility in Iran. Its sophistication suggests that it is the work of a well-financed team working for a government, rather than a group of rogue hackers trying to steal secrets or cause trouble. America and Israel are the obvious suspects. Stuxnet first came to light in June, when it was identified by VirusBlokAda, a security firm in Belarus. The next month Siemens, a German industrial giant, warned customers that their "supervisory control and data acquisition" (SCADA) management systems, which control valves, pipelines and industrial equipment, were vulnerable to the worm. It targets a piece of Siemens software, called WinCC, which runs on Microsoft Windows. For security reasons SCADA systems are not usually connected to the Internet. But Stuxnet can spread via infected memory sticks plugged into a computer's USB port. […] (Siemens says it knows of 15 plants around the world that were infected by Stuxnet, but their operations were unaffected as they were not the intended target.) […] Stuxnet was the work neither of amateur hackers nor of cybercriminals, but of a well- financed team.[3]

The unusual complexity of *Stuxnet worm* the suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals […] One or more governments (the prime suspects are Israel and America) were probably behind it. […] It is designed to infect a particular configuration of a particular type of industrial-control system – in other words, to disrupt the operation of a specific process or plant. The Stuxnet outbreak has been concentrated in Iran, which suggests that a nuclear facility in that country was the intended target."[4]

With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era?
[…] the worm eats away at a very specific kind of industrial control system: a configuration of the Siemens-manufactured Supervisory Control and Data Acquisition (SCADA) system that commands the centrifuges enriching uranium for Iran's nuclear program, the key step for an Iranian bomb […][5]

Sons of Stuxnet
A little more than one year after the infrastructure-destroying Stuxnet worm was discovered on computer systems in Iran, a new piece of malware using some of

[2] http://news.bbc.co.uk/2/hi/europe/7559850.stm, August 14, 2008.
[3] http://www.economist.com/node/17147818, September 30, 2010.
[4] http://www.economist.com/node/17147862, September 30, 2010.
[5] http://www.wired.com/dangerroom/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/, January 16, 2011.

the same techniques has been found infecting systems in Europe, according to researchers at security firm Symantec. The new malware, dubbed "Duqu" [dü-kyü], contains parts that are nearly identical to Stuxnet and appears to have been written by the same authors behind Stuxnet, or at least by someone who had direct access to the Stuxnet source code […][6]

Flame – The Flame computer virus strikes Middle East;
Israel speculation continues
A massive, data-slurping cyberweapon is circulating in the Middle East, and computers in Iran appear to have been particularly affected, according to a Russian Internet security firm. […] the "Flame" virus was unprecedented both in terms of its size and complexity, possessing the ability to turn infected computers into all-purpose spying machines that can even suck information out of nearby cell phones […][7]

Mini-Flame
A new cyberespionage tool linked to the Flame virus has been infecting computers in Lebanon, Iran and elsewhere, security researchers said Monday. Kaspersky Lab, which was credited with revealing the Flame virus earlier this year, dubbed the new malware "miniFlame," and said it was "a small and highly flexible malicious program designed to steal data and control infected systems during targeted cyber espionage operations […][8]

Examples of Cyberactions related to China in 2011

China-Based Hacking of 760 Companies Shows Cyber Cold War
Google Inc. (GOOG) and Intel Corp. (INTC) were logical targets for China-based hackers, given the solid-gold intellectual property data stored in their computers. An attack by cyberspies on iBahn, a provider of Internet services to hotels, takes some explaining. iBahn provides broadband business and entertainment access to guests of Marriott International Inc. and other hotel chains, including multinational companies that hold meetings on site. Breaking into iBahn's networks, according to a senior U.S. intelligence official familiar with the matter, may have let hackers see millions of confidential e-mails, even encrypted ones, as executives from Dubai to New York reported back on everything from new product development to merger negotiations.[9]

[6] Wired, Kim Zetter, 10.18.11, http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild/

[7] AP/ May 29, 2012, http://www.cbsnews.com/8301-501465_162-57443071-501465/flame-computer-virus-strikes-middle-east-israel-speculation-continues/

[8] Agence France Presse, Oct. 15, 2012, 1:02 PM, http://www.businessinsider.com/this-new-mini-flame-virus-is-sweeping-through-the-middle-east-2012-10

[9] http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html, December 14, 2011.

Cyber attack from China targets chemical firms
At least 48 chemical and defense companies were victims of a coordinated cyber attack that has been traced to a man in China, according to a new report from security firm Symantec Corp. Computers belonging to these companies were infected with malicious software known as "PoisonIvy," which was used to steal information such as design documents, formulas and details on manufacturing processes, Symantec said on Monday. It did not identify the companies, but said they include multiple Fortune 100 corporations that develop compounds and advanced materials, along with businesses that help manufacture infrastructure for these industries.[10]

China Hackers Hit U.S. Chamber – Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen
A group of hackers in China breached the computer defenses of America's top business-lobbying group and gained access to everything stored on its systems, including information about its three million members, according to several people familiar with the matter. The break-in at the U.S. Chamber of Commerce is one of the boldest known infiltrations in what has become a regular confrontation between U.S. companies and Chinese hackers. The complex operation, which involved at least 300 Internet addresses, was discovered and quietly shut down in May 2010. It isn't clear how much of the compromised data was viewed by the hackers. Chamber officials say internal investigators found evidence that hackers had focused on four Chamber employees who worked on Asia policy, and that six weeks of their email had been stolen. It is possible the hackers had access to the network for more than a year before the breach was uncovered, according to two people familiar with the Chamber's internal investigation. One of these people said the group behind the break-in is one that U.S. officials suspect of having ties to the Chinese government. The Chamber learned of the break-in when the Federal Bureau of Investigation told the group that servers in China were stealing its information, this person said. The FBI declined to comment on the matter. A spokesman for the Chinese Embassy in Washington, G. S., said cyberattacks are prohibited by Chinese law and China itself is a victim of attacks. He said the allegation that the attack against the Chamber originated in China "lacks proof and evidence and is irresponsible," adding that the hacking issue shouldn't be "politicized." In Beijing, Foreign Ministry spokesman L. W. said at a daily briefing that he hadn't heard about the matter, though he repeated that Chinese law forbids hacker attacks. He added that China wants to cooperate more with the international community to prevent hacker attacks.[11]

[10] http://www.msnbc.msn.com/id/45105397/ns/technology_and_science-security/t/cyber-attack-china-targets-chemical-firms-symantec/#.TzUAQF3mpaQ, October 31, 2011.

[11] http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html, December 21, 2011.

For the last few years many cyberattacks have been linked to people or computers located in China although as always it is difficult to know whether these resources were the initiations of attacks or simply relays. Very often it is very difficult to be sure of their origins or objectives as the following example, involving India, illustrates.

From the international media

Govt servers used for cyber attacks on China, other countries' networks

Investigators have unearthed a new and deadly pattern of cyber attacks in which Indian government servers have been used by foreign entities to target the computer networks of third countries. The finding comes at a time when a dispute rages within the government over who should be responsible for protecting India's critical IT infrastructure. According to sources, foreign entities have penetrated the servers of the National Informatics Centre in recent months and used them to launch attacks on countries, including China. Among other things, the NIC hosts the official websites and emails of the Indian government. "These attacks are mostly targeted against government networks of various countries," a source said, adding that the attacks were planned in such a way that investigators from the victim countries would believe that they were launched from Indian government servers. Investigators suspect foreign government entities, including intelligence agencies, have a hand in exploiting NIC servers. They say since the attacks were targeted against Chinese government servers too, there is no scope to blame China. China had in August said that it had suffered about 250,000 cyber attacks from foreign entities, 8% of which had come from India. Sources now believe these attacks could be the result of the NIC servers being exploited by foreign entities.[12]

In the following example, smartcards were the primary target of a piece of malware.

From the press

US military access cards cracked by Chinese hackers

Access to buildings and intranets harvested by super-spy Trojan. A new strain of the Sykipot Trojan is been used to compromise the Department of Defense-sanctioned smart cards used to authorise network and building access at many US government agencies, according to security researchers. Smart cards are a standard means of granting active duty military staff, selected reserve personnel, civilian employees and eligible contractors access to intranets at US Army, Navy and the Air Force

[12] http://timesofindia.indiatimes.com/tech/news/internet/Govt-servers-used-for-cyber-attacks-on-China-other-countries-networks/articleshow/10760699.cms, November 17, 2011.

facilities. They can be used to get into buildings or, when used in conjunction with a static password, to access networks.[13]

Cyber-aggression and acts of war

Among the most significant computing attacks are attacks that target a nation's critical infrastructure, for which the consequences are harmful to both that country's society and national security. If the financiers of such attacks are states, these attacks can be considered as part of a military strategy encompassing intimidation, retaliation, or offensive computing. When associated with or carried out alongside more classical military activities, such offensive computing attacks can neutralize an enemy's defences, destabilize its intelligence services, contribute to altering its decision-making process, mislead the enemy, paralyze strategic centres, or even block means of communication.

The term "cyberwar" is often misused because of its importance. Some DDoS attacks against governmental or commercial websites have been misreported in the press as acts of cyberwarfare. The term *cyberwar* should be used with caution because there is not yet any clear, consensual, universal definition of what constitutes an act of cyberwar. Does a specific attack aimed at defacing a governmental website constitute an act of war? Can this be compared to a cyberattack on the systems that controlling a nuclear power plant? Do cyberattacks need to accompany real military acts? Can a cyber-aggression be attributed clearly to a state, even if civilians perform it? Is a piece of malware comparable to an anti-personnel mine?

The notion of offensive operations that distinguish acts of war is usually tied in to the number of casualties and the amount of destruction caused. Thus, the jamming of communications and cyberattacks on air-control systems or on production facilities for essential products, such as chemicals, for example, could be considered to be acts of war. When such attacks are carried out, populations could potentially be just as affected as in the bombing of Hiroshima or in other actual conflicts.

The remote control of computers, if performed or financed by the military (the notion of military *botnets*), can be viewed as being similar to infiltrating remote-controlled soldiers. On this basis, hacking can be considered as a weapon of war, and making distinctions between the civilian and the military becomes even more difficult.

[13] http://www.theregister.co.uk/2012/01/13/sykipot_trojan_dod_smart_card_attack/, January 13, 2012.

Although massive attack scenarios are plausible, full-scale attempts have not yet been made. The existence of the dissuasive force that states possess at an international level is analogous to the nuclear deterrent. This analogy is certainly exaggerated, but the principle remains: there are a large number of states with the potential capacity to launch massive cyber-attacks or counter-attack. It would be a mistake to underestimate the potential of cyberthreats in a government's interactions, alliances, games, and geostrategic equilibriums. At the same time, however, the total destruction of the Internet through attacking the "root" servers, for example, is not conceivable because there is a real international will to prevent a massive cyberwar and to ensure the survival of the Internet. Its destruction would not be beneficial to anyone, although it might be an attractive ideal within a particular nihilist or anarchist mindset.

6.3 Cyberwar

ICT as a weapon

However, considering ICT as a weapon for offensive and defensive strategies remains a necessity, and any military doctrine should include such considerations. Most frequently, specific resources are dedicated to cyber-warfare, from strategic, tactic and operational points of view. These include:

- Cyber offensive capabilities for initiating cyber-attacks. These should primarily serve deterrent purposes by discouraging cyber conflicts and threatening activities in cyberspace.
- Cyber deterrent mechanisms including policies, postures, weapons, capabilities, or alliances.
- Cyber counter-attack strategies and tools in order to be able to use cyber-weapons against designated targets in response to an attack.
- Cyber-defense approaches, capabilities, and countermeasures in order to be able to protect assets and interests in anticipation of attacks, to protect against, to mitigate and rapidly recover from cyber-attacks. Active defense countermeasures can disrupt an attacker or redirect a cyber-attack. Malware programs can be used against the ICT resources of the enemy. A passive defense can consist of enforcing the protection of assets and cybersecurity mechanisms, for example.
- Cyber exploitation strategies and operations in order to be able to identify cyber opportunities and take advantage of them to achieve specific objectives.

- Cyber intelligence gathering, analysis and operations in order to be able to identify emerging threats before they become concrete cyber-attacks, to predict and prevent cyber conflicts, to obtain knowledge of the enemy's organisation, and to be prepared to react rapidly and efficiently to cyber attacks. Intelligence gathering relies upon any methods and techniques related to available spying activities (espionage, covert surveillance activities). Open source intelligence (OSINT) takes advantage of the Internet (and in particular, of the social web); when used in conjunction with specific cyber intelligence operations, it could help understand the environment of cyber threats.
- Cyber units, cyber warriors (organizations and competences) for offensive and defensive operations.

A key objective of cyberwar can be to disorganize the operations of the main military, industrial, economic, and administrative facilities of the enemy. ICT have changed the art of war by switching the focus onto destroying the enemy's potential for combat, to undermining the people's resoluteness, or paralyzing the enemy through Computer Network Operations (CNO) performed via telecommunication networks and information systems (Figure 6.5). In general, the global term *Computer Network Operations* includes:

- Computer Network Attacks (CAN) (cyber attacks);
- Computer Network Exploitation (CNE) (cyber exploitation);
- Computer Network Defence (CND) (cyber defence).

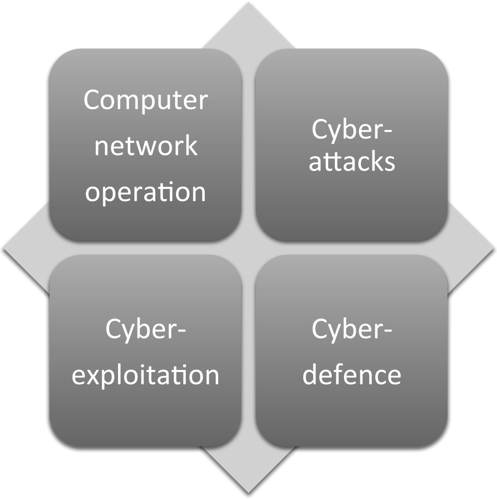


Figure 6.5 The objectives of offensive and defensive information war.

The art of war

ICT could lead to major disruptions and problems (Figure 6.6). In addition, it could add to the problems of new risks related to:

- ICT robustness, dependability, and reliability;
- ICT dependencies;
- ICT supply chain;
- Confidence in ICT manufactured in other states that could potentially be enemies of a nation.

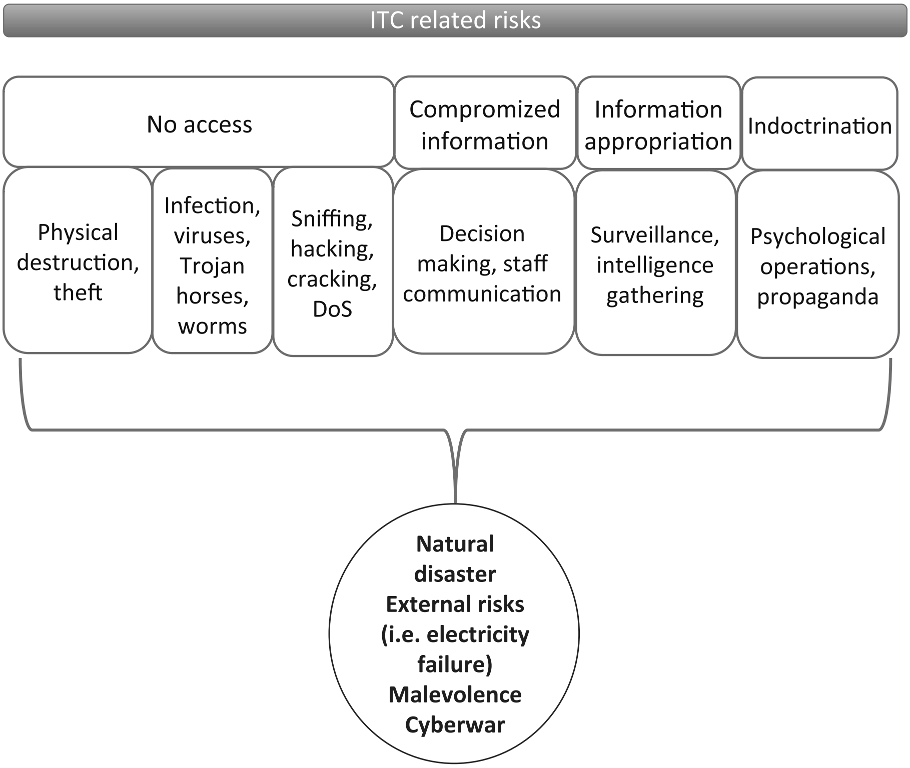

ITC related risks
No access
Compromized information
Information appropriation
Indoctrination
Physical destruction, theft
Infection, viruses, Trojan horses, worms
Sniffing, hacking, cracking, DoS
Decision making, staff communication
Surveillance, intelligence gathering
Psychological operations, propaganda
Natural disaster
External risks (i.e. electricity failure)
Malevolence
Cyberwar

Figure 6.6 ICT in a military context.

The ability to achieve victory depends on the control of information and its environment, including human and technological support. ICT are areas of innovation in waging war that provide opportunities to launch different kinds of attacks, to surprise enemies, or to adapt strategies and positions when confronted with an enemy that also controls information.

ICT also lead to war in cyberspace using information systems, software and data. Purely military skills are replaced by political, security, IT, and criminal skills. The number of front-line soldier combatants can be reduced and replaced by specialised teams (*cyber-forces*). There are no more direct confrontations and no need to physically cross geographic borders in order to invade a country.

In the same way as the air, the sea, and the land, cyberspace is a domain where military actions can take place, with the motivation of forcing the enemy to fight in a landscape where it is not ready, not equipped or not prepared. White-collar war exists in the same way as white-collar crime. A war in cyberspace might appear at first glance to be cleaner than a real war. But cyberwars are more hypocritical and more indirect (they allow the avoidance of direct confrontation); they can employ various intermediaries (technical, human and geographical); and they can have effects that are not immediately and visibly apparent and are thus more difficult to attribute to specific causes. Cyberwars can be very efficient and have impacts at different levels, such as economics, ecology, technology, media and psychology (Figure 6.7).

The use of electromagnetic impulse weapons that can prevent information processing and telecommunications in a rapid and definitive way (*technological destruction*) can be as harmful and effective as the use of chemical, biological, or even nuclear weapons, to the extent that all human activities have an increasing dependence on information technologies.

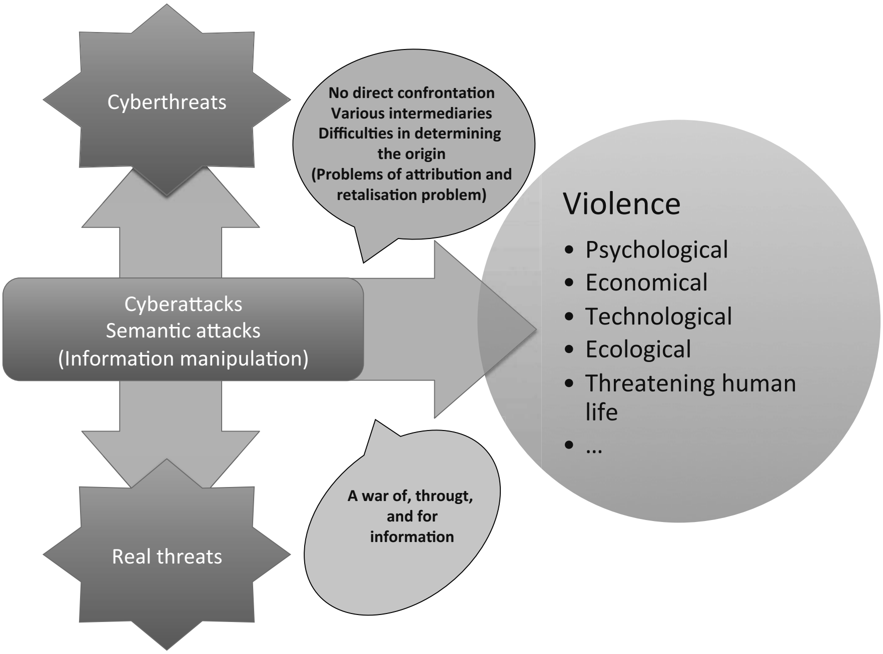


Figure 6.7 Examples of cyber-threats involved in cyberwar.

Example of a real conflict spreading over the Internet

> Hackers disrupted online access to the Tel Aviv Stock Exchange, El Al Airlines and three banks on Monday in what the government described as a cyber-offensive against Israel. The attacks came just days after an unidentified hacker, proclaiming Palestinian sympathies, posted the details of thousands of Israeli credit card holders and other personal information on the Internet in a mass theft.[14]
>
> […] Arab and Israeli hackers have taken the war online by taking down each other's websites[15].
>
> Israeli hackers brought down the websites of both the Saudi Stock Exchange (Tadawul) and the Abu Dhabi Securities Exchange (ADX) Tuesday, in the latest episode of a continuing cyber war between hackers in the two countries.[16]

6.4 Information war

Nowadays it is becoming more and more common to see attacks on web servers, governmental and other, as a means of the manifestation of disapproval. Some mercenaries, who could be doing a state's bidding, use cyberspace as a means of applying pressure. However, cyber-attacks aimed at information cannot always be compared to acts of war of genuine violence in which humans are the direct targets. Indeed, an IT attack that seeks to harm image or reputation is not equivalent to a military activity, even though it is equally an attack strategy. All military and economic conflicts can be transferred into cyberspace by means of cyber-attacks and the manipulation of information (Figure 6.8).

The Gulf War in 1990 revealed many new ways of waging war, with increased reliance on television, in particular, the news channel CNN. Millions of viewers were able to follow the war live on the screens. The armed conflict was reinforced by a media war in which information was a tool for the manipulation of public opinion.

The "Wikileaks" affair in 2010, with its exposure of certain episodes within the war in Iraq, played a smiliar role. Although the motivations were different, the end results were identical: the questioning and manipulation of public opinion.

[14] http://www.reuters.com/article/2012/01/16/us-israel-hackers-idUSTRE80F0V220120116, Janvier 16, 2012.

[15] http://z6mag.com/politics/israel-cyber-warfare-breaks-out-between-arab-neighbors-war-unfolds-in-cyberspace-164640.html

[16] http://www.haaretz.com/news/diplomacy-defense/israeli-hackers-bring-down-saudi-uae-stock-exchange-websites-1.407846, January 17, 2012.

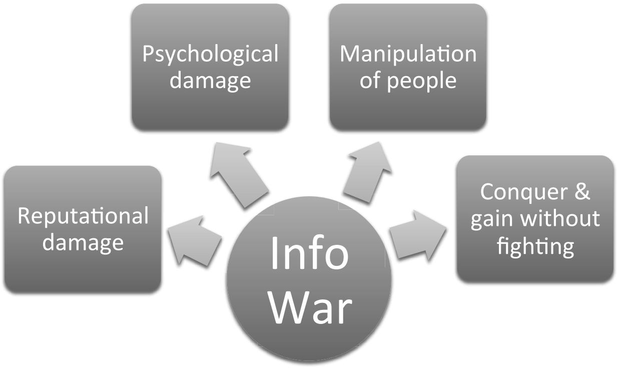


Figure 6.8 Information War (IW).

In order to win a war, it has always been necessary to control information, both strategic and operational. Nowadays it is also essential to control information on and about the war in the contexts of the media and public opinion. It is a question of managing the image of those involved and of influencing and mobilising public opinion, even recruiting "cyber-patriots" and "cyber-dissidents" who could participate in denial of service attacks on certain target systems. Discussion forums, social platforms, and other means of communication can likewise be used to support information and disinformation campaigns and spread propaganda, or to encourage and incite individuals, directly or indirectly, to commit cyber-acts of reprisal or to support real-life conflicts.

Information advantages in a military context

The importance of information, information processing, and information communication in a military context can be perceived in the terms, concepts and statements, listed in Figure 6.9, that have entered into common use.

ICT are increasingly present in weaponry and military equipment, as well as in weapon control and command systems. Information superiority comes from the ability to collect, process, analyse, and communicate information. Information superiority is the key success factor in any situation of conflict or conflict prevention.

In a military context, information and communication technologies are present in the physical domain, in the information and communication domain and in the cognitive domain (Figure 6.10). Military capabilities could be increased in several ways by leveraging the information advantages of ICT. Soldiers, traditional weapons capabilities, and battlefield equipment are increasingly being enhanced through ICT (for example, GPS-enabled guidance systems,

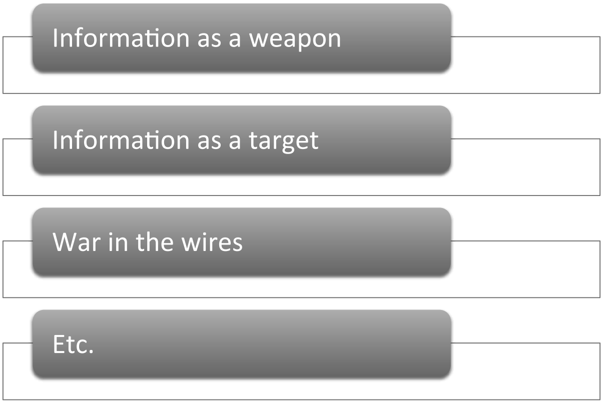


Figure 6.9 Examples of war-related expressions.

remotely controlled vehicles, etc.). It could contribute, for example, to a better understanding of situations (situational awareness), to enhanced decision support, collaboration and synchronization, and to increased precision in targeting. It could improve many functions and develop mission effectiveness and responsiveness. ICT also allows remote killing and can be used to manage cyber warfare in real-time.

The information infrastructure (contents, semantics, perception) relies upon both a technological (processing, storage and networking facilities) and a human infrastructure (Figure 6.11). Each of these can be vulnerable to, components in, or vectors of cyber-threats.

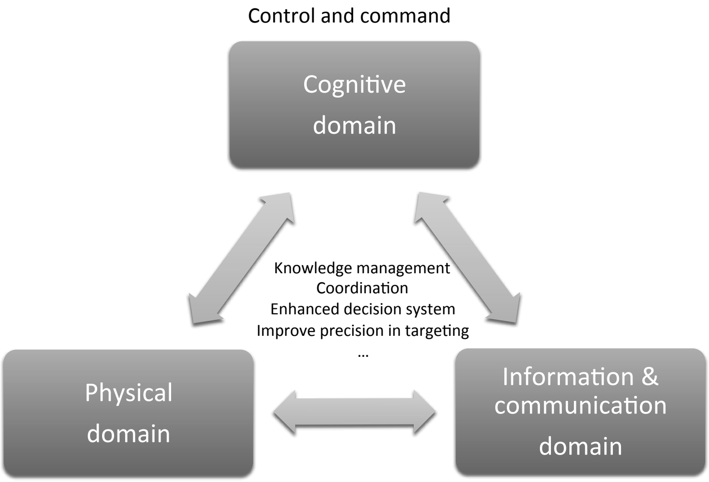


Figure 6.10 Information advantages in a military context.

For example, in the Wikileaks case, it was a soldier (part of the human infrastructure) who contributed to making the contents of secret files available to others. This could be seen as an insider agent of a cyber-threat. Without access to ICT facilities (part of the technical infrastructure), he would not have had the opportunity to record, store, and transmit information.

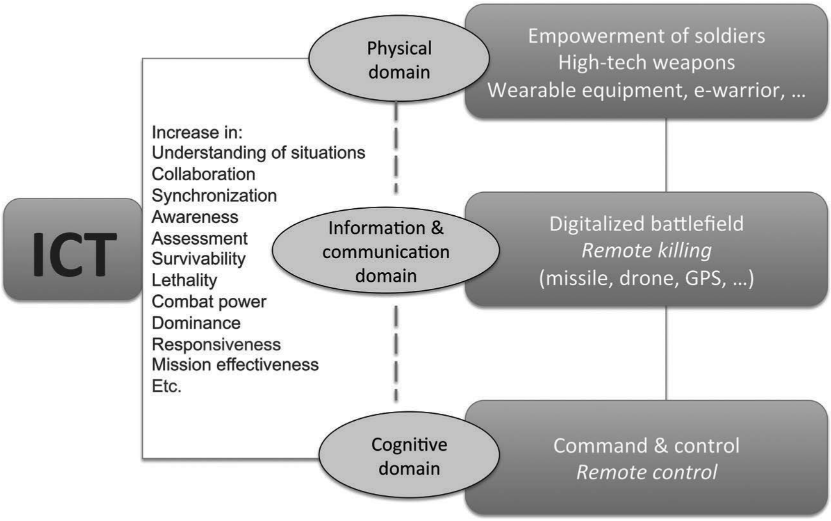


Figure 6.11 Three inter-related and inter-dependent infrastructures.

Information as a weapon

Information itself (and not only malicious software) can be a weapon, especially when it is employed in ideological campaigns designed to manipulate and influence. Psychological pressures can be applied on the enemy's military and political personnel and on its population (the notion of *psychological* or *information operations*).

Information can thus fuel conflicts and incite civilians to contribute to cyber-attacks on the sites of the enemy's government (the notion of the *civilian cyber-militia*). These propaganda activities can be encouraged by the distribution of information on the sites to attack and with instructions and tools for carrying out the attacks.

Essentially anyone with an Internet connection can use it to attack specific cross-border websites or the IT infrastructures of any other state. It is difficult to attribute any such attacks to the officials or entities within the originating state. It will always be difficult to gather formal and conclusive evidence that the state played any role in the attacks. Because of the possibility of re-routing traffic, employing multiple intermediaries, and misidentifying hackers, it is only ever possible to emerge with suggestions and suspicions of the sources of cyber-attacks. In addition, it is always possible that an individual or a group of individuals would claim responsibility for the organisation of a cyber-attack as some kind of personal protest.

The mobilisation of civilians can be extremely rapid and efficient across cyberspace and can use all the standard information media (radio and television channels, possibly even banking networks). In wartime, just as in peacetime, any kind of telecommunication or information networks can be converted into an *Offensive Information War Unit.*

According to this principle, cyberspace and information can contribute to inciting civil disobedience and can harm democracy. At the same time, the Internet can make it easier to draw attention to attempts to subvert democracy. The definition of "cyber-rebellion" and of what it covers depends on the context in which it is used. For some, cyber-rebellion is an act of war or a gesture of support for those opposing an existing regime, while for others it is a manifestation of the freedom of expression.

The events of the Arab Spring of 2011 bear witness to this. The insurgent protest movement that became visible through physical demonstrations was also active in cyberspace, notably by means of the Anonymous group, which has existed since 2003. This group was able to mobilise public opinion by such acts as:

- defacing websites, leaving behind evidence of their visit along the lines of text such as "we are anonymous, we are legion, we do not forgive, we do not forget, expect us";
- launching denial of service attacks on sites, leaving them unavailable and causing them to malfunction or simply stop working for shorter or longer periods;
- stealing and publishing confidential information.

Some examples of Anonymous' actions from the headlines

NYSE.com suffers blips as Anonymous takes aim.[17]

Anonymous gain access to FBI and Scotland Yard hacking call – Hacking network Anonymous has released a recording of a conference call between the FBI and UK police in which they discuss efforts against hackers.[18]

[17] http://money.cnn.com/2011/10/10/technology/anonymous_nyse/index.htm, October 10, 2011.

[18] http://www.bbc.co.uk/news/world-us-canada-16875921, February 3, 2012.

Hackers leak Assad's astonishing office emails – Hundreds of emails from the office of Bashar al Assad have been leaked by the hacker group Anonymous.[19]

About Anonymous from Anonymous Analytics' web site

Who We Are
Anonymous is a decentralized network of individuals focused on promoting access to information, free speech, and transparency. The group has made international headlines by exposing The Church of Scientology, supporting anti-corruption movements in Zimbabwe and India, and providing secure platforms for Iranian citizens to criticize their government.

Anonymous Analytics, a faction of Anonymous, has moved the issue of transparency from the political level to the corporate level. To this end, we use our unique skill sets to expose companies that practice poor corporate governance and are involved in large-scale fraudulent activities.

What We Do
We provide the public with investigative reports exposing corrupt companies. Our team includes analysts, forensic accountants, statisticians, computer experts, and lawyers from various jurisdictions and backgrounds. All information presented in our reports is acquired through legal channels, fact-checked, and vetted thoroughly before release. This is both for the protection of our associates as well as groups/individuals who rely on our work.[20]

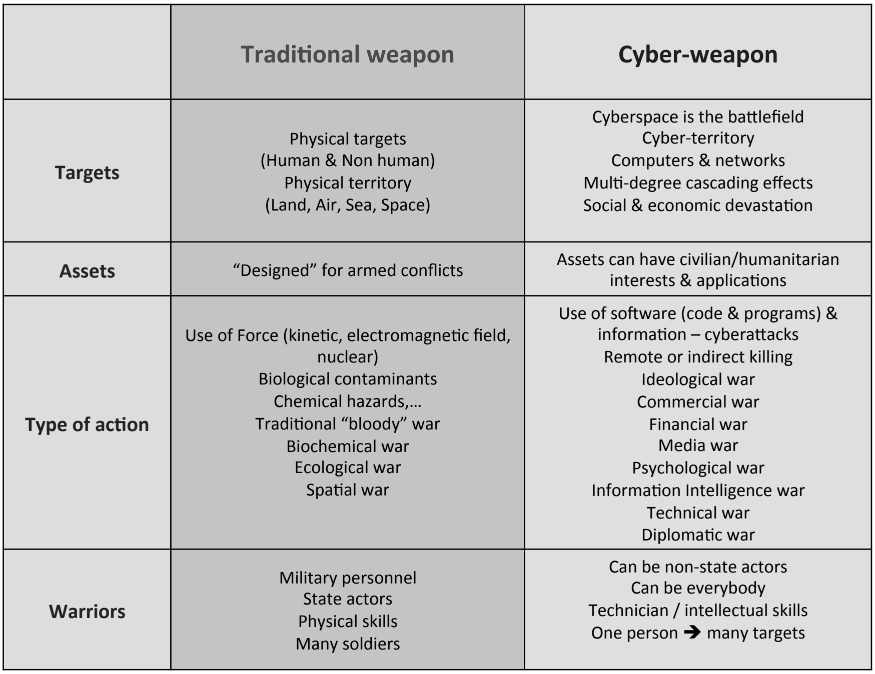
Hacktivism is a form of protest that uses information, and sometimes malware, to further political objectives, and foster and sustain civil disobedience. The ICT resources of decision makers can be targeted by hacktivists in order to protest against their policies. Patriotic hackers can equally launch cyber protest attacks, such as DDoS or defacement attacks, against the governmental sites of foreign countries. Through cyberspace, civilians can become full-fledged participants in military conflicts and thereby serve their countries. Individuals can carry out information warfare. Certain states have understood the advantages to be drawn from having a population trained in the use of ICT and have recruited the experts that they need for military, diplomatic, or political purposes from their populations. At the same time, they have obtained the

[19] http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9067118/Anonymous-hackers-leak-Syrias-Bashar-al-Assads-astonishing-office-emails-discussing-Barbara-Walters.html, February 10, 2012.

[20] http://anonanalytics.com/

technical and technological skills that were lacking (and were necessary to meet their objectives) by recruiting from the cyber-criminal community.

Figure 6.12 Summarises the principal differences between traditional weapons and cyber-weapons



	Traditional weapon	Cyber-weapon
Targets	Physical targets (Human & Non human) Physical territory (Land, Air, Sea, Space)	Cyberspace is the battlefield Cyber-territory Computers & networks Multi-degree cascading effects Social & economic devastation
Assets	"Designed" for armed conflicts	Assets can have civilian/humanitarian interests & applications
Type of action	Use of Force (kinetic, electromagnetic field, nuclear) Biological contaminants Chemical hazards,... Traditional "bloody" war Biochemical war Ecological war Spatial war	Use of software (code & programs) & information – cyberattacks Remote or indirect killing Ideological war Commercial war Financial war Media war Psychological war Information Intelligence war Technical war Diplomatic war
Warriors	Military personnel State actors Physical skills Many soldiers	Can be non-state actors Can be everybody Technician / intellectual skills One person ➔ many targets

Figure 6.12 Main characteristics of traditional weapons versus cyberweapons.

In addition, military forces take advantage of ICT. They have naturally moved into cyberspace to acquire intelligence and perform monitoring or spying. The Internet allows the dissemination of propaganda and the manipulation of public opinion in order to justify aggression or defensive acts, or even to incite people to act on nationalist reflexes. The power of the Internet as a communications tool need not be demonstrated. Conflicts can be stirred up and aggravated by Internet users transformed (at least in their own minds) into cyber-patriots who, driven by the intention to damage a particular community, can saturate websites hostile to their cause and orchestrate campaigns of misinformation. Attacks coming from all around the world, often remote-controlled and automated, can be hard for the victims to stop.

It is not always easy to attribute acts of computing war to a specific state or to prove its direct or indirect responsibility; this is due to the proliferation of the technical intermediaries, mercenaries, or *botnets*. Additionally, it is hard to launch an Internet attack without passing through infrastructures in allied or neutral countries. The potential participants in a global cyberwar are not isolated because the entire infrastructure is interconnected and interdependent.

Responding to cyber acts of war

It is always difficult to identify the persons responsible for launching cyberattacks, whether these are politically or criminally motivated, unless the authors actually claim responsibility. The latter is often the case with terrorist attacks. Perpetrators want to attract or gain visibility both to enhance the impact of their actions and to present their claims. At the opposite end of the spectrum, criminals prefer discretion. In political conflicts the ambiguity and uncertainty of cyberattacks are often preferred. If a state can avoid the possibility of the clear attribution of responsibility for cyberattacks to their agents, this makes it difficult for the country that was attacked to aggressively retaliate, physically or electronically. Cyberattacks should have "sufficient gravity" to be considered as armed attacks.

The attribution of responsibility is a crucial issue for the international community. It raises several legal questions. One current debate concerns whether cyberattacks are essentially a criminal matter, and thus subject to domestic criminal law, or acts of war to which international laws on warfare should be applied[21]. The Laws of War require the attribution of an armed attack to a foreign government before responding with force.

[21] "Laws of War" refers to several Conventions, Treaty and Protocols. Among these we can quote the following:
Hague II Convention (1899); Hague IV (1907): Laws and Customs of War land
Geneva Convention (1864): Amelioration of the condition of the wounded on field of battle;
Geneva Protocol (1928) For the prohibition of the use in war of asphyxiating gas and for bacteriological methods of warfare.
Geneva Convention revised in 1949:
Geneva Convention I: For the amelioration of the condition of the wounded and sick in armed forces in the field
Geneva Convention II: For the amelioration of the condition of the wounded, sick and shipwrecked members of armed forces at sea
Geneva Convention III: Relative to the treatment of prisoners of war
Geneva Convention IV: Relative to the protection of civilian in time war
Geneva Convention (1975): Prohibition of the development, production and stockpiling of bacteriological and toxin weapons and their destruction
Protocol I (1977): Relating to the protection of victims of international armed conflicts
Protocol I (1977): Relating to the protection of victims of non-international armed conflicts
Protocol III (2005): Relating to the adoption of an additional distinctive emblem

The point is to determine whether the country that has been attacked has the right to respond to an act of cyberwar, using either passive defences or active cyberdefence measures against the ICT infrastructures of the other state. This could include the right to use cyberattack countermeasures not only against the state at the origin of the cyberattacks but also against all the intermediary states that passively allowed, or contributed to, the attacks and neglected to prevent, knowingly or not, the cyberattacks from within their national borders. Sometimes active defence could be viewed as a form of reprisal and be used as self-defence in anticipation of a real attack.

As yet there is no international treaty, convention, or protocol that address this question or the question of how to distinguish a criminal cyber-attack from a military cyber-attack. Individual states are thus free to interpret their rights on the basis of their own legal corpus and culture, taking into account guidance from existing international laws and the means by which states have long relied to solve their disputes peacefully. If only criminal laws should apply, that would mean the countries do not have the right to use active defence, such that their defence relies solely upon their capacity to prevent and deter cyber-attacks (passive defence). This is insufficient from the perspective of military doctrine, especially given that cybercriminals can act with impunity from the shelter of digital paradises and that some countries are not sufficiently enough active in respect of the prosecution or extradition of cybercriminals. Deterrence based on criminal law raises the problem of the effectiveness of both law enforcement and international cooperation when dealing with international cyber-attacks. Within their national territory, states should prevent (and not encourage) the perpetration of cyber acts of war against other territories and refrain from providing any form of support to individuals to commit such acts, if the state wishes to avoid the risk of being held (indirectly) responsible for such acts. The same principle applies to the state's attitude towards cybercrimes.

6.5 Cyberterrorism: a particular kind of cyberconflict

The terrorist dimension of cybercrime

Currently the definition of cyberterrorism is not at all clear. The easiest definition would be to consider it as terrorism committed in cyberspace. In common usage, however, terrorism refers to the systematic use of violence for a political objective, and it is appropriate to ask whether the unavailability or malfunctioning of the Internet as a result of malicious acts would be capable of terrorizing the population. Would it not be more relevant to revise the definition to cover economic terrorism targeted at damaging and disrupting organizations, commercial and financial institutions, or governmental agencies that carry out part of their activities on the Internet? Are there any innocent victims? Economic (cyber) terrorism is just a specific form of very strategically targeted terrorism, the objective of which is to create feelings of insecurity in a targeted community. Rumours can also spread fear and generate chaos in cyberspace that could influence economic, diplomatic, or political activities in the physical world.

It is necessary to be careful with the use of the word "cyberterrorism," which has been employed in its current sense since 9/11. The first distributed denial of service attacks (DDoS) that affected the websites of Yahoo, CNN, and eBay on February 10, 2000 were carried out by a teenager who was identified and arrested a few months afterwards. Even though his motivations were not made public, there is no reason to suspect that they were political. But what if the same attack had been carried out after the fall of the World Trade Center? Would such an attack have been considered as cyber-terrorism? Without any concrete elements, such as a list of demands or the identity of the originator of an attack, it is hard to define an attack as being an example of cyber-terrorism or to determine the motivations and objectives of the single or multiple perpetrators.

Some cybercrime activities or cyber-attacks can have a terrorist dimension to the extent that the systems under attack are components of critical infrastructures. Indeed, infrastructures that are essential for to the smooth running of a country's activities (energy, water, transport, food supply logistics, banking and finance, medical services, administration services, telecommunication infrastructures, etc.) immediately became more vulnerable with the generalization of Internet technologies in every sector of activity. Electricity production and distribution systems underpin the effective operation of most of the other infrastructure elements.

Attacks on the systems that control electricity production and distribution are also aimed at affecting public safety by causing panic, creating terror, and endangering the survival of human populations. In some circumstances, in particular in the energy domain (electricity, nuclear power plants, or water treatment systems), the transportation domain (telecommunication networks, rail networks, aerial control) and the health domain (hospitals, medicine production), taking control of these facilities could well be a key objective of cyberterrorism. The unavailability of such infrastructures for any period could lead to malfunctions in, or interruptions to, indispensable services and to financial or even human losses. Attacks against financial systems or the manipulation of public opinion could lead to reactions that contribute to the collapse of the financial system, thereby harming the economy of a whole country through the loss of credibility and investments. A possible scenario could be that an accidental disaster (explosion of a gas main) or a classical terrorist act (explosion of a bomb) took place. Associated with cyberattacks that prevented the organization and mobilization of help (causing, say, the unavailability of telecommunication networks or of the fire brigade call centre), these circumstances could certainly lead to a significant increase in human losses.

If an individual or a group, within or outside a big entity that is a pillar of the national economy, could manage through computing attacks to completely block that entity's operations, this could destabilize a country. Taking an organization's computing resources hostage in order to blackmail it and causing its activities to cease temporarily is not unknown in the field of computing terrorism. The direct and indirect negative impacts of such attacks can be disastrous over a long period. It is not necessary to be a terrorist to blackmail an organization by threatening to hijack or make unavailable its computing resources or actually make them unavailable, as is shown by the following case in which computing resources were taken hostage by a system administrator in San Francisco in 2008. The network administrator of the network held the city's FiberWan network hostage.

From the media

Net Admin Accused of Locking down San Francisco FiberWAN System

The San Francisco Chronicle reports that officials say T. C., a 43-year-old computer network administrator, created a password that granted him exclusive access to the city's new FiberWAN. The system contains records such as officials' e-mails, city payroll files, confidential law enforcement documents and jail inmate bookings. He is charged with four counts of computer tampering. The story says he gave pass codes that didn't work to police and refused to divulge the true code, even when threatened with arrest. City officials are working to regain access to the system, though they say breaking through his denial of access to other system administrators could cost millions of dollars. The story quotes an unnamed source saying that T. C. had been disciplined recently for poor performance and his supervisors tried to fire him. It also says he had set up a monitoring system to alert him if anything changed in his personnel matter and that city officials worry that he might have passed to a third party information that would allow the system to be hacked remotely.[22]

[22] http://www.itbusinessedge.com/cm/community/news/gov/blog/net-admin-accused-of-locking-down-san-francisco-fiberwan-system/?cs=19824, July 15, 2008.

Links between the criminal and terrorist worlds

It is possible to suggest a difference between the motivations of crime and terrorism in cyberspace. This difference would lie in the nature of the expected benefits for the perpetrators. For one group it would be enrichment, while for the others it would be the exercise of political pressure through visible acts as spectacular as they are terrifying. If only the target is known, it is sometimes difficult to distinguish the motivations of a delinquent, a terrorist, a mercenary, a militant, a fraudster, or a simple spoiler. The type and nature of an attack is not a sufficient basis for determining with any certainty the motivations or objectives of perpetrator. Additional information is always required.

The cyberterror threat can be understood in a broad sense, but the concept is vague and badly defined, and frequently, as is the case for the term “cyberwar,” the term “cyberterrorism” is misapplied. The distinction between cybercrime and cyberterrorism is not clear, and the words are often confused.

The Internet can link the criminal and terrorist worlds, especially in financial dealings. The criminal world sees in terrorism a source of profit and a potential means of obtaining power. The criminal and terrorist worlds collaborate in cyberspace to attain financial goals and share technical competencies. Terrorists use the services and competencies of (cyber-) criminals to finance their activities (both contributing to the acquisition of financing and generating the sums needed for their projects) and to have access to the computing power that they require (Figure 6.13).

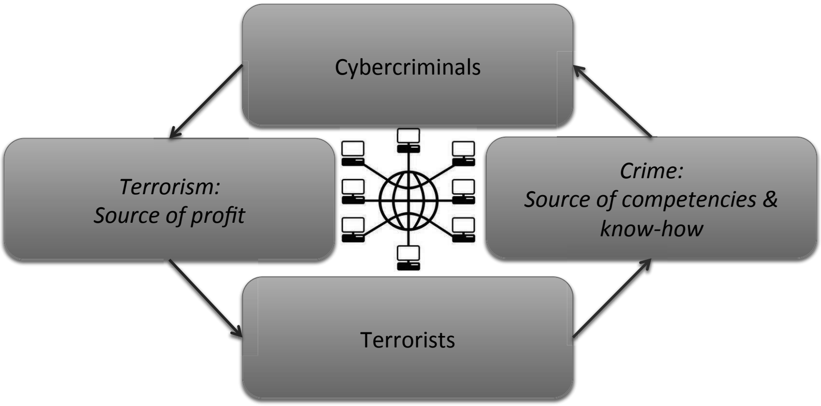


Figure 6.13 Correlations between terrorism and crime.

For example, the rent or purchase of malware and botnet networks can make it possible for terrorists to:

- hack and gain access to computer systems;
- attack computer systems seen as symbols and, therefore, as targets to destroy;
- deform websites and publish messages;
- carry out spectacular attacks with the goal of increased media attention;
- cause panic in order to destabilize;
- create diversions to real-world attacks;
- attack and damage the physical environment (the computer centres of chemical factories, for example);
- carry out combined attacks in the physical world and in cyberspace.

Terrorists use the Internet as an efficient communication tool to, among other activities, share and publish propaganda and intelligence, recruit, train, raise and transfer funds, look for targets, organize and plan operations and communicate.

The Internet can multiply the criminal and terrorist capacities of individuals, even if they are not computing professionals. Nowadays, the Internet can be seen as a tool to enhance, enforce, and foster any terrorist activities, and sometimes even to enable them. For example, applications Google Maps, Google Earth or Google Street View offer to all users, including terrorists, all the information and pictures necessary to identify potential targets with impunity, without having to visit physically the sites. Google makes available pictures of zones that can be sensitive. Google allows users to consult plans, identifying the most vulnerable and most symbolic infrastructures, nerve centres and access points, and potential obstacles or countermeasures.

The terrorists can find in cyberspace everything they need to make a success of their plans, and thus the Internet is a valued strategic asset for terrorists. It allows them efficient organization and leadership (an international organisation, networked and with a horizontal structure, is both possible and more difficult to counter), rapid and anonymous communications, simple transfers of funds, efficient intelligence gathering, broad dissemination of information, and a means of recruiting members. Via cyberspace, small groups of terrorists can gain a global presence.

As in political campaigns, terrorists manage and control their image through the Internet and promote their ideology through carefully documented information websites or social platforms. Collaboration and communication tools can help them to foster the spirit of their motivation among their followers, supporters or general public, and maintain their fervour. Terrorist information campaigns could be seen as a kind of white–collar terrorism (Figure 6.14).

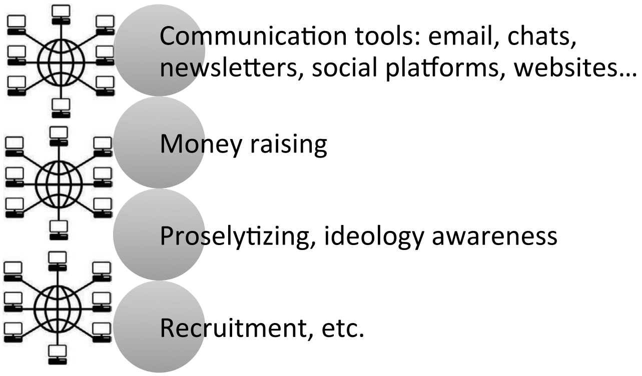

Communication tools: email, chats, newsletters, social platforms, websites…
Money raising
Proselytizing, ideology awareness
Recruitment, etc.

Figure 6.14 Internet as an enabling tool for terrorists.

A question of interpretation

It is necessary to be extremely careful about the origins of computing attacks that harm symbols and are reported as the work of cyber-terrorists, because the events could be part of a wider effort of manipulation. There is a fundamental difference between the theoretical possibility of an attack and actual performance of such an attack. There is a lack of quantitative elements that can be used to study the real extent and the nature of cyber-attacks, a field that is in constant evolution. Without reliable knowledge, it is difficult to evaluate the problem correctly and precisely. It is always possible to over- or underestimate the reality of cyber-attacks. This undermines the abilities of authorities to develop, effectively and efficiently, strategic and operational cybersecurity counter-measures. Moreover, it leaves the way open to all kinds of irrational approaches to security, based on potential multi-form threats that are often synonymous with fear rather than based on reality.

The security and control measures implemented within the framework of the fight against international terrorism have more significant consequences for the general public, affecting a greater number of people in their daily lives, than any acts of terrorism itself.

6.6 Cybercrime or cyber conflict?

Towards more cyber attacks

Both public and private companies often risk having their resources and information stolen and their communication networks penetrated. They also run the risk of being the victims of hackers, sometimes as part of coordinated attacks on sensitive infrastructures. These risks must be taken seriously as potential threats to competitiveness, reputation, and, to a larger extent, to state sovereignty, national or public security, and democracy itself.

As a result of the opportunities available for carrying out cyberattacks, with the expected growth in the scope, sophistication, and consequences of these attacks, cyberspace should be considered as a risky domain for all of its users. As we have seen, the risks concern not only nation-states, but also all private and public organisations and individuals. Because of the high correlation between the political, economic, and social stakes and challenges in real life and in cyberspace, and the huge economic competition that exists in a interconnected and globalized world, state-level cyberthreats, cyberattacks or cyberhostilities can be a tactic to develop supremacies and hegemonies or to dispute cyberterritories in cyberspace. It could contribute to controlling enemies (economic or political) in a kind of "cyber Code War." Although it seems unlikely that a real cyberwar is ongoing, this does not mean that a new spiral of cyberactivities is not emerging.

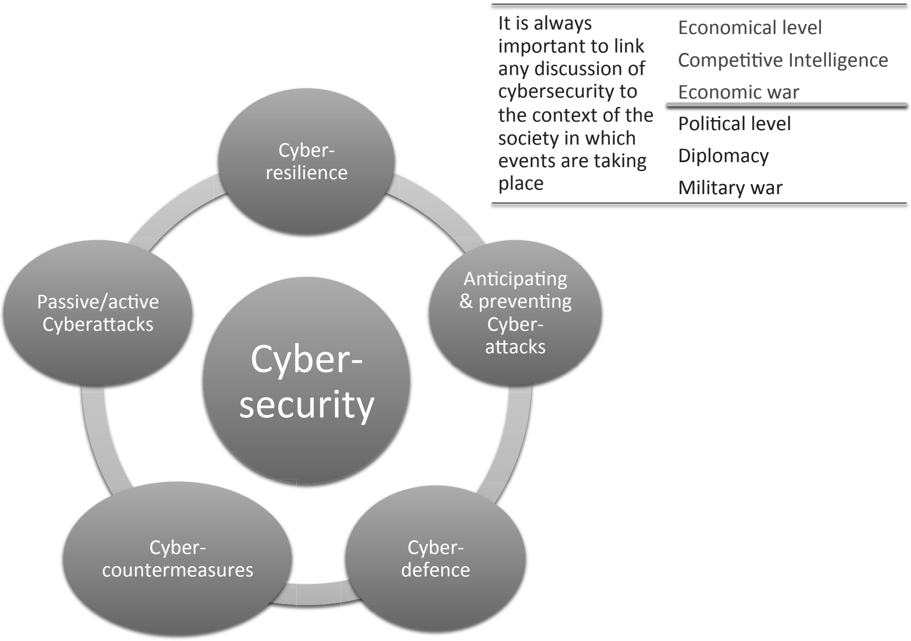
States have to develop and enforce the robustness and resilience of ICT infrastructures, and, at the same time, they need to enhance their means of anticipating and preventing cyber attacks and to develop means of (potentially) attacking their enemies. This leads to the emergence of a new form of power: cyberpower. From now on, cyber-attacks and cyber counter-measures will be part of national defence systems and military doctrine. These include all forms of passive cyber attacks, such as espionage and intelligence information gathering, and are not limited to offensive and destructive cyber attacks (Figure 6. 15).

Towards more stability in cyberspace: a shared responsibility

For the well-being of the digital society, a real political willingness at national and international levels is needed to stop the arms race in cyberspace (or at least to restrict it to an acceptable threshold), and to ensure that cyberspace is not destroyed or altered by unfair practices or by intense competition.

Cyberspace should be considered as an essential, open, global common resource and should benefit from international treaties designed to contribute to reducing accidental or deliberate cyber-incidents and cyber-attacks, regardless of their originators (individuals, recreational hackers, militants, extremists, hacktivists, criminals, militaries, governmental or private institutions).

"Cyber war," "information war," "offensive or defensive cyberwar" – these are all terms used to describe conflicts that are both economic and military in nature. These terms raise issues of our responsibility (at an individual, national, and international level), of international cooperation, and of the necessary partnerships between the private and public sectors.


Cyber-
resilience
Anticipating & preventing Cyber-attacks
Cyber-
defence
Cyber-
countermeasures
Passive/active Cyberattacks
Cyber-
security

It is always important to link any discussion of cybersecurity to the context of the society in which events are taking place	Economical level Competitive Intelligence Economic war
	Political level Diplomacy Military war

Figure 6.15 The response to cyberthreats and means of cyberdefence.

6.7 Summary

The homeland security of states is now being confronted with criminal threats linked to the existence of information technologies. These technologies and the Internet are at the heart of the information war (*infowar*), the stakes of which are primarily economic. As we have seen, the Internet not only allows the manipulation of information, but also provides a privileged tool for spreading rumours, disinformation, or propaganda designed to destabilize. It also makes aspects of espionage much easier, because it has become reasonably simple to intercept or to access amounts of information transferred over the Internet. What seems the most harmful, because unverifiable in an absolute sense, is the semantic war (war through information), of which the damage is not directly observable. A war linked to symbols can support intimidation that generates fear and thus contributes to the effectiveness of cyberterrorism. The invisible character of the threat makes it even more dangerous.

Cybercrime is directed at individuals, organisations, and nations. The impacts of these crimes vary according to their victims, but cybercriminality can be defined as an information technology war that uses information to acquire information. Cyberspace is the new battlefield for economic and military warfare. Information technologies and telecommunications infrastructures are the targets for delinquency, organised crime, terrorism and conflict." Information technologies are more and more involved in power struggles, profiteering, intimidation, threats, takeovers, destruction, surveillance, the manipulation of information for exemple. They are used as the means of striking those targets and have become the tools of crime, terrorism, and warfare.

6.8 Exercises

1. In what way can cyberattacks against critical infrastructures be more serious than physical attacks?
2. Why is it necessary for organizations to protect themselves against attacks aimed at their SCADA (Supervisory Control and Data Acquisition) systems?
3. To what does the term "Digital Pearl Harbor" refer?
4. What are the principal cyberthreats applicable to the military domain?
5. What are the main differences between cyberattacks related to criminal, terrorist or military activities?
6. From a legal perspective, what is the main distinction between a cyberattack with criminal origins and one that constitutes an act of war?
7. Is it ever possible to be completely certain about the source of a cyberattack? Why is this the case, and what problems does it cause?
8. In what ways have terrorists gained headway in cyberspace?
11. At a national level, what are the risks linked to the wrong interpretation of the sources of a cyberattack?
12. What are the defining characteristics of the Anonymous group?
13. How does Anonymous recruit its members?
14. Which tools of cyberattack does Anonymous employ?

Chapter 7

Understanding Cybercriminals

7.1 Understanding the context

In order to prevent, detect, pursue or punish cybercrimes, it is necessary to understand the profiles and the motivations of cybercriminals. Understanding a hacker's motivation and level of technical skills can help assess how serious an attack is and assist in devising an appropriate counter-strategy. To secure an information system, it is necessary to know against whom it needs to be protected.

The preceding chapters have shown that cybercriminality is within the power of virtually everyone. There is a vast range of motivations and knowledge among cybercriminals, and the ways of expressing these are many and varied. Because of this, it is difficult to provide an exhaustive list of possibilities or to present a rigorous classification of cybercriminals.

A first approach is to classify cybercriminals into two main groups: the professionals who make money or any kind of profit from their work, and the amateurs.

7.2 Towards a classification of cybercriminals

A distinction based on profits

The professionals earn a living from these clandestine revenue-generating activities, while in contrast, the amateurs are more often searching for social recognition or have found an amusing way to pass time or play games online.

This distinction is far from adequate for a precise categorization of the whole field of cybercriminality, but it allows us to distinguish most of their motivations.

Professional criminals generally fall into one or more of these categories:

- any criminal elements connected or not to organized crime;
- direct competitors of the organization targeted;
- civil servants;
- mercenaries (hackers in the pay of an organization in the private or the public sector).

Amateur criminals may fall into a number of other categories.

- Technicians; these can in some sense be viewed as the descendants of the original "hackers." They can be computer or security experts. Some are motivated by the desire to display their mastery of the technologies or by the search for glory. Others want to contribute to improving the robustness of technologies or solutions or to identify and remediate vulnerabilities or backdoors implanted in security products;
- Snoopers and the curious;
- Pranksters, also called "script kiddies" or "kidiots," who frequently enjoy a great amount of publicity. The fact that they tend to be the criminals most frequently unmasked should not lead us, however, to imagine that they are the only type of hackers;
- Minor criminals, people with nothing to do, people looking for revenge, people looking to demonstrate their power, people wanting to join a gang, voyeurs, etc.;
- The mentally ill or psychologically disturbed individuals, egotists, people addicted to digital technologies, etc.;
- Activists or terrorists working not for money but for an ideological, political or religious cause, or national pride (frequently more professional than purely amateur, or a combination of both).

At the most basic level, cybercriminals are simply criminals who use the Internet for their purposes. They are no different from traditional criminals of the kind we have always known. They are looking for criminal opportunities and, when they find them, they exploit them according to their abilities or the abilities of other criminals with whom they can join forces to commit specific cyberattacks (Figure 7.1).

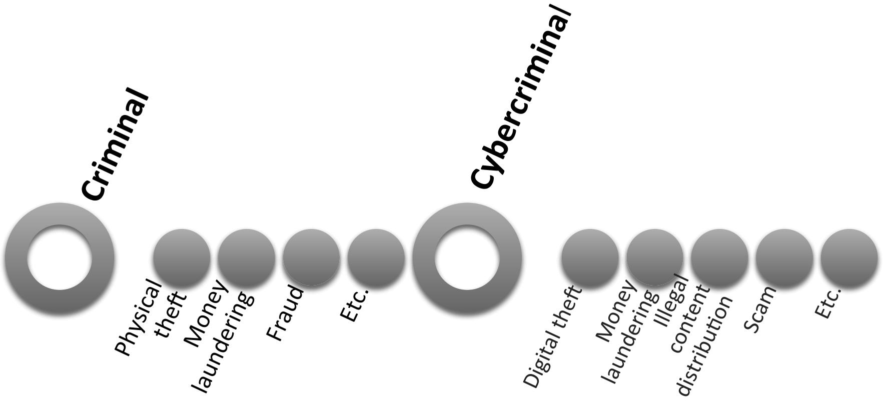


Figure 7.1 Cybercriminals: criminals like any others.

They have adjusted to the information society and have optimised their way of working to take advantage of the possibilities that the Internet offers. The Internet has changed the game in terms of criminality by widening the potential market to include every Internet user and every organisation with an Internet presence (because the Internet itself, the computers, source code and data can all serve as the means of crimes). The Internet has also allowed the development of new kinds of crime, with computers or data as targets.

A typology of motivations

Participants in cybercriminality can be distinguished according to criteria related to their motivations. The underlying motivation of these individuals may derive from social, technical, political, financial, political, or government-related factors (Figure 7.2).

Social factors are typically the need for peer recognition, often linked to membership in a gang or group. These hackers want to demonstrate their importance by living up to the group's values. Their acts are analogous to those of urban graffiti artists, and are based on a very simplistic view of a social hierarchy. This is frequently the case among pranksters who engage in hacking because it gives them a feeling of superiority and control over institutions that they perceive as dominating in ordinary life.

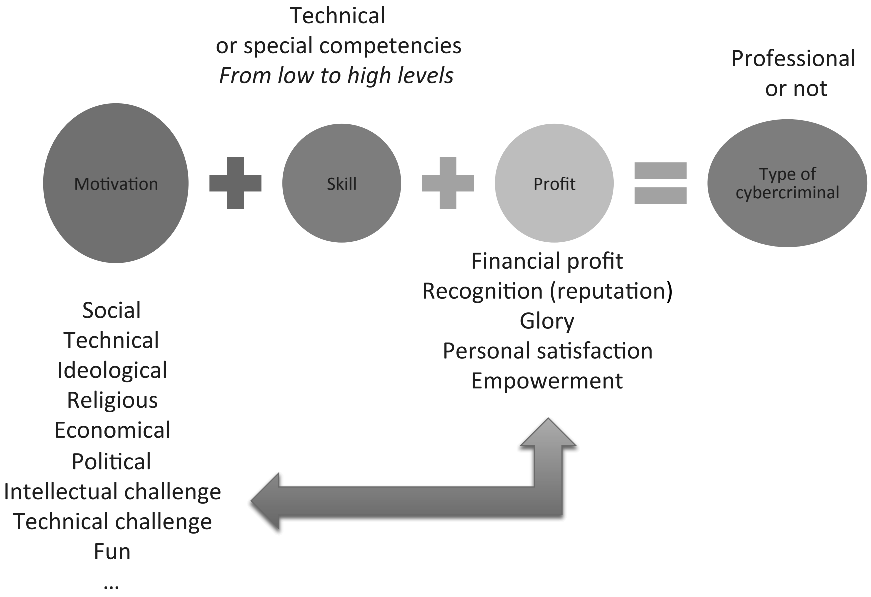


Figure 7.2 Example of criteria to enable the classification of cybercriminals.

Social motivations usually find their roots in the need of recognition by others, usually bounded by the structure of a group. Collective emulation, the psychology of belonging: here as in other social groups each individual wants to prove his value to the group with reference to the internal cultural criteria. A common characteristic in such groups is the immaturity of those involved, very often populated by individuals for whom hacking is an opportunity to control an organisation that they believe is treating them unfairly.

Technical motivation has the primary objective of exploring the limits of a technology, demonstrating those limits and vulnerabilities, and understanding the strengths.

Political motivation focuses on events that will attract media interest so as to draw attention to a serious problem, in order to build public awareness leading to its resolution. The dividing line between this and terrorism may be thin or vague, at least in theory. It is not uncommon for a socially-motivated individual to hide behind a political goal.

Financial motivation can be a strong factor, and underlies a large number of illegal actions. The lure of easy money draws white-collar criminals (fraudsters, embezzlers, criminal competitors, etc.) to ply their trade on the Internet. Delinquents and criminals have been able to adapt themselves to new technologies to continue and expand their traditional activities. It is legitimate to be worried when we see how creative they can be when they invent new criminal uses.

In the interest of being exhaustive, we should mention, even though they do not fall into the categories of cybercriminals, the military entities that can participate in cyberconflicts. In cyberspace, the distinction between traditional criminal acts and warfare is unclear and difficult to establish, mainly arising from the fact that criminals and militaries employ the same IT weapons, the same toolboxes to carry out cyberattacks and achieve their objectives.

Cybercriminals fit into a wide variety of profiles. In addition, the dynamic nature of the Internet, the constantly renewed criminal opportunities that it offers, and the evolving behaviours of both Internet users and criminals, taken together mean that it is difficult to catalogue these profiles in any definitive way.

In order to be effective, cyberattacks can:

- exploit weaknesses in software for which security solutions have not yet been developed or applied (0-day exploits);
- exploit vulnerabilities of security solutions.

It is in manipulating legitimate uses of commercial solutions, or knowing their limits and vulnerabilities, or having previously hacked them, that criminal cyberattacks on chosen targets will be successful.

Arguably, the companies that occupy monopoly positions with operating systems, software and irreplaceable web services (such as, for example, Adobe, Microsoft, Apple, Google and Facebook), or in the field of security solutions (such as, for example, RSA Security, Symantec or Kaspersky Labs), are despite themselves indirectly linked to the world of cybercriminality. To a certain extent they can be vectors of cybercriminality that contribute to both its spread and its targets.

At the same time these monopolistic entities are capable of developing counter-attacks or other security counter-measures and playing a role in dissuading attackers, in contributing to detecting and stopping cyberattacks, and in identifying the participants in cybercriminality.

For a long time, the motivations of cybercriminals were mainly notoriety, publicity, intellectual challenges, and peer recognition. Nowadays, cybercriminals are more motivated by profit than by glory, power, or personal satisfaction. Cybercriminal organizations and cybergangs operate all over the world. A summary of cybercriminal motivations is set out in Figure 7.3.

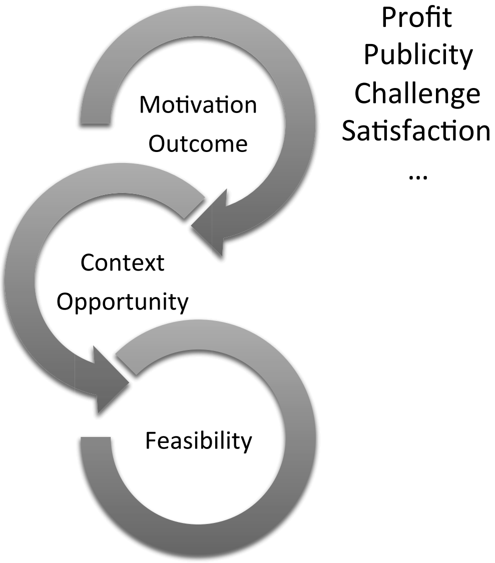


Figure 7.3 Various motivations for cybercriminality.

Example from Reuters

Inside a Global Cybercrime Ring
Innovative Marketing Ukraine, or IMU, was at the center of a complex underground corporate empire with operations stretching from Eastern Europe to Bahrain; from India and Singapore to the United States. A researcher with anti-virus software maker McAfee Inc. who spent months studying the company's operations estimates that the business generated revenue of about $180 million in 2008, selling programs in at least two dozen countries. […]

The company built its wealth pioneering *scareware* – programs that pretend to scan a computer for viruses, and then tell the user that their machine is infected. The goal is to persuade the victim to voluntarily hand over their credit card information, paying $50 to $80 to "clean" their PC.

Scareware, also known as *rogueware* or *fake antivirus software*, has become one of the fastest-growing, and most prevalent, types of Internet fraud. Software maker Panda Security estimates that each month some 35 million PCs worldwide, or 3.5 percent of all computers, are infected with these malicious programs, putting more than $400 million a year in the hands of cybercriminals. […] Groups like Innovative Marketing build the viruses and collect the money but leave the work of distributing their merchandise to outside hackers. Once infected, the machines become virtually impossible to operate. The scareware also removes legitimate anti-virus software from vendors including Symantec Corp, McAfee and Trend Micro Inc., leaving PCs vulnerable to other attacks.

> When victims pay the fee, the virus appears to vanish, but in some cases, the machine is then infiltrated by other malicious programs. Hackers often sell the victim's credit card credentials to the highest bidder.
>
> Removing scareware is a top revenue generator for Geek Choice, a PC repair company with about two dozen outlets in the United States. The outfit charges $100 to $150 to clean infected machines, a service that accounts for about 30 percent of all calls. […] Anti-virus software makers have also gotten into the lucrative business of cleaning PCs, charging for those services even when their products fall down on the job […].[1]

Beyond profit and motivations: how can cybercriminals be classified?

From the ordinary citizen to the true criminal, there is a wide range of people who could behave as cybercriminals. Beyond a classification based on profits or motivations, or a distinction drawn along purely legalistic lines, we can usefully attack the problem by asking a number of key questions, such as:

- Who are these people?
- What objectives do people have when the publish information on the Internet such as, for example, recipes for making illegal products such as drugs?[2]
- Is somebody who illegally downloads music or movies a cybercriminal? From the point of view of the law, certainly, as is shown by the conviction of this American housewife sentenced to pay the music industry 1.9 million U.S. dollars. "*Woman fined to tune of $1.9 million for illegal downloads* – A federal jury Thursday found a 32-year-old Minnesota woman guilty of illegally downloading music from the Internet and fined her $80,000 each – a total of $1.9 million – for 24 songs."[3]

For this lawsuit to go ahead, her cyberactivities needed to be watched, tracked and reported. In order to do so, the relevant governmental institutions, police, and private security agencies presumably use the same techniques as

[1] http://www.reuters.com/article/2010/03/24/us-technology-scareware-idUSTRE62N29T20100324, 25 March 2010.

[2] If the two key words *make ecstasy* are entered in a search engine, this last returns about 63,400,000 results in 0.17 seconds and about 2,640,000 results in 0.11 seconds for the key words *make date rape drug* (Feb. 2012).

[3] http://articles.cnn.com/2009-06-18/justice/minnesota.music.download.fine_1_jury-instructions-fined-sheryl-crow?_s=PM:CRIME, 18 June 18 2009.

cybercriminals in performing their work albeit in a structured and managed framework. Was this woman in the last example, the victim of cybermonitoring abuse?

In fact, professional cybercriminals rarely face justice. Their very real mastery of the technologies they use, alongside their understanding of the Internet and police investigations, means that they are frequently able to leave very few traces of their activities or cover these traces effectively. Even when these traces are identified, it is rare that the criminals can be clearly identified. "Hiding" on the Internet is still possible for a competent person. We can also ask ourselves who is the guiltiest party: the user of a piece of software to jailbreak a DVD, or the person who created or distributed it?

Is the ordinary citizen a victim or a criminal? Is it unfair to depict the user of some services available on the web, even when he knows they are forbidden, as also being a victim in some small way? He is surely victim to the extent that he does not know that he is being watched, when he does not care about leaving traces or how to conceal them. The Internet is now part of everyday life. It highlights the true nature of human beings. Becoming a victim or a criminal, based on the services offered on the Internet, has now become both a possibility and a reality.

Parallel to this, the facilities for harassment or surveillance that the Internet and, in particular, smartphones, provide to users can prove a great temptation for the jealous, the suspicious, and the generally malicious, to the detriment of those around them.

Numerous sensors, devices and services that are in daily use are constantly recording personal geo-data. This can be done either with the explicit consent of the users (GPS, smartphones, social networks, web applications, etc.) or without. There are numerous applications that make use of geo-data, including applications for military, police, marketing, and personal usage, such as retrieving a stolen smartphone, locating a missing elderly person or a hiker lost in the mountains, monitoring a convicted criminal, sending ad hoc information to combat troops, helping people to meet each other through social applications, city-guide applications, geolocalized and personalized marketing, supply chain management, etc.

The evolution of the quasi-systematic use of geolocalization data has allowed the localization and tracking of individuals and has introduced new possibilities for surveillance and espionage by both legitimate bodies and less welcome users of the data – usually without their knowledge.

Potential problems related to the collection and use of all these data include the fundamental principle that all of these applications contribute to monitoring and profiling people wherever they are, and that at any instant, the data being generated can also be used by anyone else for any purpose. It is easy to transform a smartphone into a "spy-phone" that allows a third party to listen to all that is said nearby, reading SMSes and emails, reading and deleting the data contained in the smartphone, etc.

In the absence of legal constraints and effective countermeasures, the collection and processing of geo-data can be misused in order to perform real time monitoring of people and activities and to carry out breaches of privacy that could then lead to other, more concrete, offences against people.

Is it legitimate to consider entities that misuse such monitoring capacities as, to some extent, cybercriminals? It seems inevitable that these problems will grow because everyone is increasingly using "intelligent" tools and more efficient sensors of various kinds, and also because an increasing number of efficient systems for managing and analyzing these huge amounts of geo-data are being designed, developed and used for financial profits. There is a real need for balance between the added value to individuals and society provided by geo-tagging services and the risks to privacy that arise from the potential misuse and abuse of their data.

Example

Suspicious spouses log into cyber crime

Jilted lovers, jealous boyfriends and girlfriends and even married men and women, from good financial and educational backgrounds, are increasingly getting involved in cyber crime to "get even." They are doing all this to spy on the persons they have known up close and personal.

Cyber crime cell senior superintendent of police K.V.P.S. said, "There have been incidences where the ex-boyfriend of a girl was sending obscene messages to the new boyfriend of the girl from a fake e-mail address. These people are highly educated and can work their way around a computer." He said in most cases of privacy invasion, it is either the spouse of the victim or someone who is intimately known to them. […] An official of cyber crime wing said suspicious husbands and wives also indulge in password hacking to check for clues of straying behaviour exhibited by their spouses.[4]

[4] http://articles.timesofindia.indiatimes.com/2011-06-29/chandigarh/29716851_1_cyber-crime-spouses-boyfriend, 29 June 2011.

7.3 About hacking and hackers

Activities and behaviours

The word *hacking* finds its roots in the vocabulary of cooking, originally meaning the chopping up of ingredients. By extrapolation, it now applies to activities that consist of dissecting the operating processes of a computer, in order to understand every single element and, possibly, to misappropriate them.[5] There is a difference between understanding the limits of security and searching for defaults, and then exploiting them in order to perform malicious acts. But the boundary can sometimes be too small or the temptation too great.

In the absence of a formal typology of cybercriminality, there is a distinction to be made between people genuinely enthusiastic about information systems and criminals or swindlers. Hackers are often real experts in information

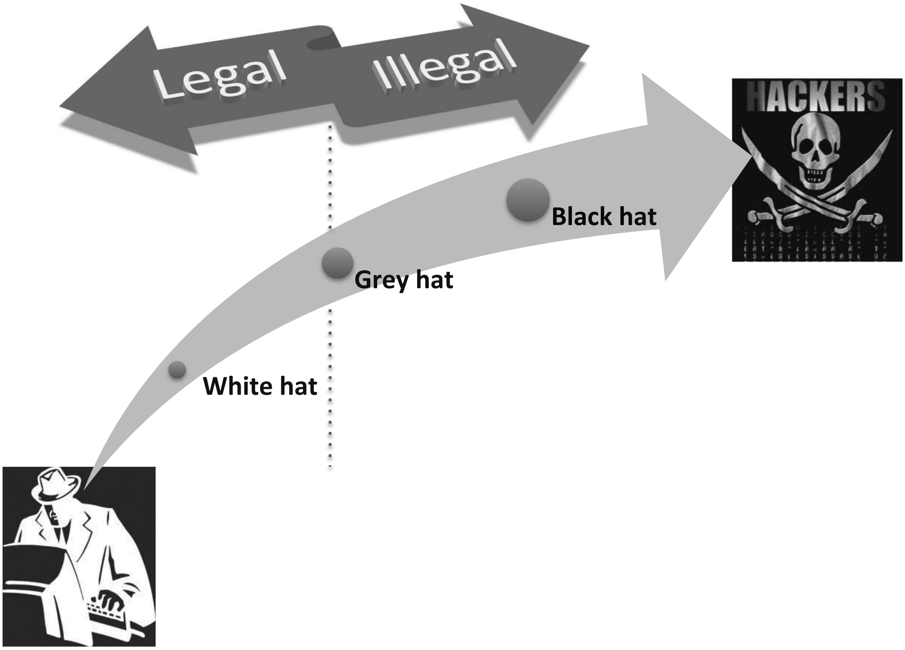


Figure 7.4 Different kinds of hackers.

[5] The first definition of "hacker" given by the New Hacker's dictionary is: "A person who enjoys exploring the details of programmable systems and how to stretch their capabilities." See http://www.outpost9.com/reference/jargon/jargon_23.html#SEC30

technology, networks, telecommunications, computer security, and cryptography. Their motivations, sometimes but not always creditable, can vary as a result of their socio-cultural or socio-professional memberships. Depending on their ethics and the uses to which they apply their knowledge (at the service or not of society, licit *versus* illicit), it is common to describe hackers by the colour of a hat, in reference to the hat worn traditionally by cowboys.

Even though it is rare that hackers identify themselves in this way, a *whitehat* is associated with the good ones, those who work towards better security through legitimate and licit activities (in fact these are security experts), while *blackhats* are the misusers of technologies and systems. Extending the analogy, we can also talk of *greyhats* as hackers who, depending on the circumstances, are sometimes white, sometimes black (Figure 7.4).

A greyhat example

> *The greyhat-IS-whitehat List*
> The people listed in this list consider themselves apart of the "hacker-underground." They have become public figures in the security-industry yet they all have a burning desire to stay in "the hacker underground." Most of the companies these people work for make claims that they don't hire "hackers." Keep in mind the people in this list are "Whitehats" but consider themselves grey. They help the security industry and continue to help manipulate others (either directly or indirectly) to follow in their footsteps. People who consider themselves "Greyhats" that are not in the public eye or do not publicly contribute to the security-industry will not be listed. Watch out for companies who hire these people. This list is far from complete[…] this is all public info.[6]

We can also classify a *blue hat* as an expert in hacking Windows and a *red hat* an expert in hacking UNIX.

The hacking community, always on the lookout for new talent, could describe itself effectively using the slogan *"seek and you shall find."* It gravitates towards and around websites that are created and then disappear as a consequence of interest in particular subjects and of the hide-and-seek games being played by the stakeholders.

Often the hackers who are caught are those looking for social recognition and who accordingly boast of their exploits on the Internet, or those, as the example below illustrates, who make no effort to hide their identity.

[6] http://www.digitalsec.net/stuff/website-mirrors/pHC/old/greyhat-IS-whitehat.txt, 14 February 2012.

Example from real life

The Homeless Hacker v. The New York Times – A self-styled security expert and serial self-promoter, Adrian Lamo made headlines as a grayhat hacker.

Lamo is one of the best-known hackers in the country, and was out being filmed for a documentary when the cops came looking for him at his parents' house in Sacramento. While cameras rolled, Lamo described his most famous hacks, a string of highly publicized computer intrusions – Microsoft, AOL, and Excite@Home – of which the Times was merely the most recent.[7] Just months before the Times hack, he had made the papers by burrowing into WorldCom's intranet, where he found a database containing Social Security numbers, bank account data, and direct deposit instructions for some 86,000 WorldCom employees – plus a Web router maintenance tool that enabled him to go deep into the private networks of Bank of America, Citicorp, and JP Morgan.

Known as the Homeless Hacker before his arrest, Lamo did most of his virtual exploring from the Internet connections at Kinko's copy shops. Besides his laptop – an eight-year-old Toshiba with six keys missing – he traveled light, usually with a blanket, a change of clothes, and a Taser stun gun, which he used to pick electronic locks and sometimes to shock vending machines to see if they would drop food or spare change.

Relentlessly nomadic – he has crossed the country by bus half a dozen times – he's also a connoisseur of serendipity. He once spent two weeks attending a Pennsylvania Bible school on a whim. Mostly, though, he transited between Washington, DC, and San Francisco, where he grew up. Because he has friends in those cities, Lamo could usually count on finding a place to sleep that was both more secure and more pleasant than his usual home, an abandoned building. The capital also has the virtue of being an information hunter's paradise. "In DC, it's hard to open a dumpster without finding classified documents," he tells me wistfully.

For someone with such a glamorous hacking resume, Lamo is strangely unschooled. Illiterate in computer languages like Java and C++, he cannot exploit loopholes in a system's underlying code. Instead, he uses a common man's tool: the Web browser. Firing up Internet Explorer, Lamo will troll through a corporation's homepage, seeking outsourced jobs like advertising, distribution, and payroll. The companies that handle these tasks link to the main corporate database, but their proxy servers – the point of connection between the two networks – are often poorly secured, sometimes with standard-issue passwords that no one bothers to reset.

Finding these weak points is a matter of perseverance more than talent, but Lamo has also been unusually lucky – often materializing in areas of corporate networks that were heavily guarded and distinctly off-limits. One fellow hacker describes the skill – with a nod to sci-fi author Neal Stephenson – as "the ability to condense fact from the vapor of nuance. [...] Grayhats see themselves as Internet Zorros – high-minded vigilantes who are righteously setting information free while nobly

[7] The greyhat hacker Adrian Lamo was arrested in 2003.

> helping to protect it from vandals. In practice, though, it can be hard to tell the noble outlaw from the petty criminal. Breaking the law in the name of improving the law is rarely condoned, let alone idealized. The line between self-interest and "setting information free," moreover, is easily blurred – and it's the murky middle ground in the already ill-defined grayhat arena where Lamo most likes to operate […] In theory, it's easy to see Lamo as a good guy. Unlike many hackers – even whitehats – he never uses a pseudonym and makes no effort to hide his identity. If the company he notifies appears grateful, he will often offer to help plug the hole he's discovered for free […][8]

The terminology of hackers

The term *hacker,* in its common, pejorative sense that is today synonymous with criminal, refers to a person who gains unauthorized access to computer or network systems through programming skills, computer knowledge, and tools. A hacker's objective is to gain knowledge about computers, network systems or security mechanisms, and then use this knowledge to prepare and launch an attack, whereas a *cracker* is more interested in just gaining unauthorized access to servers or networks. Thanks to their programming skills, hackers often prepare their attack by creating code or exploiting vulnerabilities that have been found. A hacker who prepares, creates, and launches an attack often has personal pleasure as a motive. They often target servers or networks with high profiles and high security. They like to find flaws and to write viruses or malicious code exploiting these security vulnerabilities. The feeling of belonging to a group also motivates hackers. Belonging to this community enables them to share their experiences, their knowledge, their skills, and their techniques, and to get peer recognition.

It is common that the information systems of governmental agencies, as much as private organizations, attract white hat, grey hat, or even black hat hackers for all kinds of operations (monitoring, spying, information, search for people, information manipulation, launching cyberattacks, securing their information systems, testing the robustness of their security solutions, etc.).

Some hackers do not have the choice to collaborate with the police, while some do it for free and others are paid.

[8] http://www.wired.com/wired/archive/12.04/hacker_pr.html

Example

> *Ex-hacker testifies about reporting U.S. Army leaks suspect*
> A former computer hacker testified on Tuesday that he led authorities to the suspected source of the biggest leak of classified documents in U.S. history after several days of online chats with Bradass87, an alias for Army intelligence analyst Bradley Manning. The 24-year-old Manning is charged with downloading thousands of classified or confidential files from the military's Secret Internet Protocol Router Network, or SIPRNet. Those files are thought to have later appeared on WikiLeaks, a whistleblower website. Former hacker Adrian Lamo said Manning initially contacted him by email in May 2010 and the two began an online conversation about diplomatic cables and military video the Army private allegedly downloaded from the classified network he used as a member of the 10th Mountain Division in Iraq. [...] Lamo's testimony came on the fifth day of a military hearing to determine whether there is sufficient evidence to court-martial Manning for aiding the enemy and other charges in connection with the massive leak of documents. He faces life imprisonment if convicted of the most serious charge. [...] Lamo said he confirmed the identity of Bradass87 by becoming friends with Manning on Facebook and by confirming that he had a password and login for the Army's online knowledge portal. Lamo, who pleaded guilty to the felony hacking of The New York Times' computer system in 2004, acknowledged under cross-examination by Manning's attorney that he is a minister in the Universal Life Church and had told the person in an online chat to "treat this as a confession." [...] Computer crimes investigator P. E. said Lamo gave authorities a removable computer hard drive, a laptop and two thumbdrives with details from his chats with Manning [...].[9]

There are no official or widely accepted definitions of the terms crackers, cyberdelinquents, cybergangs, script kiddies or nerds. In order to provide a framework of definitions, however, we present below, without any pretence of being exhaustive or authoritative, a number of factors that can help characterize the people or activities related to cybercriminality.

Crackers are people who break, disable, remove or circumvent security mechanisms. In general, they have malicious or criminal intentions. They could be independent or belong to direct competitors of the targeted organization, or even state employees. Some could be gangsters or mercenaries acting for private or public institutions.

A *cybergang* is often composed of a group of criminal hackers who individually acquired the programming skills allowing them to transfer their criminal activities from the real world to the virtual world. These cybergangs are

[9] af.reuters.com/article/worldNews/idAFTRE7BK05G20111221, 21 December 2011

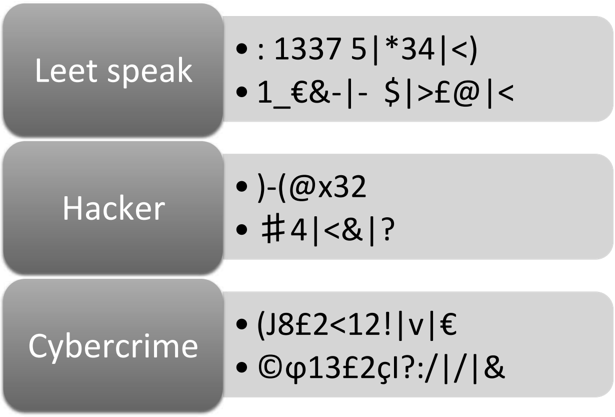
often based in countries that do not have the necessary legal framework to combat cybercrimes. The real threat coming from the cybergangs is their ability to possess high-level skills, to be coordinated, to have a worldwide scope, and to plan and execute long-term attack strategies.

Cyberdelinquents more often are amateurs, whose motivations are social, technical, political or sometimes – more rarely – financial, and who can see themselves as technical wizards inspired by the desire to master more and more technologies. To give only two examples, they can be rebellious Internet users or unsatisfied employees.

A *script kiddy* (SK) is an unsophisticated, novice attacker. As the script kiddies do not have sufficient knowledge to create their own attacks or viruses, they use existing and easy-to-find techniques, lists of written commands, hacking manuals, do-it-yourself virus kits, programs, or scripts to search for vulnerabilities and to exploit these security breaches. They often prefer to scan thousand of individual computers to find weaknesses instead of taking the time to find exploits in advanced systems. Thus, they focus on a small number of vulnerabilities, but they scan the entire Internet to find these exploits. The real threat coming from the script kiddies is the fact that any inexperienced computer user can freely download malicious programs available on the Internet and then use them to attack vulnerable machines or networks.

Due to their passion for information technology and the Internet, some hackers are sometimes qualified as *geeks*. They distinguish themselves from crackers and script kiddies, who are young/new crackers. The script kiddies can also be identified on a pejorative way as being *nerds*. A *nerd*, young or not, is passionate about technology, and often displays some kind of social ineptitude, but with a relatively limited knowledge of computing, especially in respect of programming. Nevertheless, he or she likes speaking in a computer jargon commonly known as *leet speak*, (derived from the word elite) that was restricted at the beginning to the elites of programming. Leet speak is a writing code where the characters used are graphically close to our alphabet, replacing for example a by 4 or @, e by 3, the s by a 5, x by ><, h by)-(, etc. (Figure 7.5).

A *nerd* or a *script kiddy* uses usually pre-built tools, existing malicious software, in order to carry out attacks and to have fun shutting down most vulnerable systems, usually chosen randomly. The cracking and hacking community often disavows *script kiddies,* or *kidiots*, who are sometimes identified as simply being a new kind of hooligans. They can be harmful to the extent that they are numerous and because of their availability and doggedness, dedicated to causing damage by trying scripts or testing the robustness of systems



Leet speak

- : 1337 5|*34|<)
- 1_€&-|- $|>£@|<

Hacker

-)-(@x32
- ♯4|<&|?

Cybercrime

- (J8£2<12!|v|€
- ©φ13£2çl?:/|/|&

Figure 7.5 Leet speak.

in order to identify and attack the weakest. For the hacking contests aimed to *geeks*, only a moderately high level of technical knowledge is needed, because such events are designed to be recreation activities where the tests are created to allow participants to have fun, just like a Sudoku. Moreover, the average age in these contests is younger than in, for example, Defcon,[10] where much greater skills are required in order to pass the tests.

7.4 Hackers' conventions, contests, and school

Of late hacking has entered the spotlight. Many hacker conventions take place around the world, offering the possibility for skilled people to show their performances and to get recognition from their peers. Among the most famous are: Black Hat Briefings,[11] Defcon,[12] Chaos Communication Congress – (Chaos Computer Club),[13] and the Hack In The Box Security Conference.[14]

A utopian search for absolute knowledge remains the common objective of the hackers. This can be a kind of challenge against themselves, against their own limits, and can look like a time trial to be the first to identify and exploit a fault. If the main motivation is not necessarily financial enrichment, the desire

[10] http://www.defcon.org/

[11] www.blackhat.com/

[12] www.defcon.org/ (around 8000 people attended, their 19th convention in Las Vegas in 2011).

[13] www.ccc.de/congress (oldest and bigger European hacker convention held annually in Germany).

[14] www.conference.hackinthebox.org (Asia's largest annual network security conference, which were held every year in Kuala Lumpur (Malaysia) and more recently in the Middle East).

of power of some kind, such as recognition by peers, is the driving force for their activities. The proof of this is in the existence of big international hacking contests, real demonstrations of exploits in the fields of breaking security protection and demonstrating knowledge of information technologies, in which many of the best hackers and security experts take part.

The most famous hacking contest is certainly the one that has taken place every summer since 1993 in a casino in Las Vegas: the almost mythical CTF (*Capture The Flag* organized within the framework of the Defcon. The word *Defcon* refers to a measure of alert of the American military forces (*DEFense readiness CONdition*).

The expression *Capture the flag* refers to American games, multimedia or non-multimedia, where the objective is to capture and to plant a flag, symbolically in the same way as the first man on the moon on July 20, 1969. The exploit of hacking consists then of resolving enigmas and getting into computer systems as fast as possible.

It is interesting to reveal that there are fewer spectacular announcements of software cracking or of the discovery of new vulnerabilities during Defcon. White hat hackers have a tendency not to reveal or publish their discoveries, because the big software houses, such as Oracle, Microsoft, and Cisco, for example, systematically complain about violations of their licences, which forbid reverse engineering, an essential method for analysing software.[15] In some cases, at best, these major corporations recognize the origin of the discovery by mentioning the name of the hacker who discovered it. It should be noted at this juncture that this type of unpublished discovery (known as a *zero day*) could be sold on the black market for several thousand dollars.

In 2011 there was for the first time a Defcon kids contest.[16] That constitutes a turning point and emphasises the importance of the need for young people with high technical skills. Defconkids can promote the idea that hacking is a game and natural leisure activity, that anybody can do it, and that hacking should be part of all educational programs to be an effective and educated individual in the 21st century.

Making the young believe that hacking is a legitimate and useful pastime can make it difficult to help them understand the distinction between what is

[15] To give only one example, Dmitry Sklyarov was arrested by the FBI after giving a presentation called “eBook’s Security – Theory and Practice” in the Defcon-9 conference 2001 for having circumvented copyright protection measures related to the “eBook Reader” produced by Adobe Systems, Inc. under the terms of the Digital Millenennium Copyright Act. (*“Russian crypto expert arrested at Def Con”* – http://news.cnet.com/2100-1001-270082.html; July 17, 2001).

[16] “DEFCON Kids was part of DEFCON 19, the largest hacker gathering in the world.” Source: http://www.defconkids.org/

legal, authorised, and tolerated and what is illegal or immoral. This can be exacerbated by the fact that within the framework of Defcon, it is adults coming primarily from a professional environment, who organise and perform the demonstrations of hacking and explain the techniques. It can be a double-edged sword to reinforce their taste for hacking, for exploits and innovations in the domain of misusing technologies, or to encourage the search for weaknesses, by presenting hacking as a legitimate and valuable activity. Not all who learn the lessons will go on to become security professionals working in a legal environment.

In fact this kind of event can help public or private entities or agencies to identify at an early stage potential hackers with young competencies in the hacking field (potential future enemies of society) or valuable future collaborators to work in ICT security, law enforcement, national security, or defence.

Schools specialized in information and communication technology warfare or hacking techniques already exist in several countries. They can be integrated in either military or engineering schools. Depending on the schools and their objectives, the goals of these programs could be to train cybersoldiers, skilled engineers and technicians for offensive and defensive cyberwarfare, cybersecurity experts, or a hacker elite.

Example

For nearly 20 years, a school for hackers, specialized in electronic warfare, has had the objective of creating a hacker elite.[17] This military academy teaches its students to write computer viruses, to penetrate network systems, and to program weapon guidance systems. It is said that they graduate around one hundred cybersoldiers every year, and that the hosting country possesses a cyberwarfare unit of six hundred skilled members, hackers, and technicians.[18]

7.5 Portraits of hackers

Example of a young hacker's attitude

An example of a young hacker's experience taken from an anonymous interview from Frontline and his related "story" from the U.S. Department of Justice:

[17] www.globalsecurity.org

[18] www.strategypage.com

The interview

Q: What is it about the computer that makes it become such an obsession for young guys?
R: Well, it's power at your fingertips. You can control all these computers from the government, from the military, from large corporations. And if you know what you're doing, you can travel through the Internet at your will, with no restrictions. That's power; it's a power trip. *Why is that so important?* Well, everybody likes to feel in control. *In my time, they did it by playing hockey or football. How does the computer compare?* It's intellectual. It stimulates my mind. It's a challenge. [...]

Q: When you start out, you sort of poke at various cyberfences and walls. You're just looking for the soft spots. You don't target a place because it's got something that you want – it's just that it's a challenge?
R: I would target a place because it looks like a challenge. Like, if I say, "The navy has a computer network in Jacksonville, maybe that would be fun to poke around." And then I'd target them. I'd look at their computers and I'd see what I can do there.

Q: That doesn't sound like mischief. Sometimes I think you guys are like the graffiti spraypainters.
R: Not at all. Well, first of all, I was just looking around, playing around. What was fun for me was a challenge to see what I could pull off. But then there's other people that go into corporate web sites, government web sites, and change it. That's closer to what you're talking about – that's mischievous. But I didn't do stuff like that.

Q: You could have, though.
R: Oh, yes. I could have gotten a lot of recognition. [...]

Q: A lot of attention was given to the fact that you downloaded software relating to the international space station. Could you have done anything with that?
R: No. It was for the environmental control program. Who wants that – you can play with the air conditioner, or what? [...] The code itself was crappy [...] certainly not worth $1.7 million like they claimed. The only reason I was downloading the source code in the first place was because I was studying C programming. And what better way to learn than reading software written by the government?

Q: When did you first suspect that they knew you were snooping around?
R: Well, I never knew that they would actually come to my house. That was a total shock to me. Sometimes I would get kicked off a computer, and I'd figure, "Oh, great, the admin figured something was up and re-installed the software, added a little security, and forgot about it, because they don't care that I'm here. They just fix it and move on," which is reasonable. Nothing happened to me in the weeks following, so, great. They realized that all it takes is five minutes at the keyboard and they can make a computer secure. And they didn't care. I would email the system administrators sometimes and tell them that their computers were

vulnerable. I would tell them how to break in, and how to fix the problems. I'd give them advice, and they would never follow it. Three weeks later I would go in and I still had access to their computers.

Q: Even after you told them that there's a hole in the fence?
R: Oh, more than that. I told them how to fix the hole in the fence, and they didn't respond, so I figured that they didn't care.

Q: How did they catch you?
R: They haven't told me exactly how they caught me. They sealed the affidavit for the search warrant. They said it was sealed for national security or some BS reason, but from what I understood, they probably called one of my friends, who gave information about me. Then they came to my house. My mom woke me from bed and said that the FBI was at the door. It's kind of unnerving. […] I walk out and I see everybody with vests that say Federal Agents and NASA and DOD on the back with guns and all that good stuff.

Q: Were you scared?
R: No, I was just wondering what was up, and then I saw that their shirt said NASA.

Q: And they walked out with all your computers?
R: They took me into a room in the back and questioned me for a few hours. And I admitted everything that I did, and I said, "Yes, I'm sorry. I won't do it again." I told them how I did it, what I did. They told me not to do it again, and if I do it again, I'll leave in handcuffs, but for now, they don't consider me a criminal, and that I just shouldn't do it again. And then they told me that they're taking my computers for investigative reasons. They said they don't need to read me my Miranda rights because they're not making an arrest. They're just investigating.

Q: So what did they take out of there?
R: They took five of my computers. I had a nice little network going. They took my Palm Pilot, my CDs, my "Star Trek" book.

Q: And when did it get serious?
R: I didn't hear from them for another three months. Then, three months later, they had a little meeting. I talked to the prosecuting attorney. They said they might press charges. He said that I might get probation […] but that they were unsure of what they're going to do. Then, in July, over the summer, I was in Israel. And I got a phone call from my father, who said that they wanted to put me in jail for six months.

Let's think about it from the other side's point of view. They don't know that it's some nice guy from a nice neighborhood. […] It could be a real bad guy in Baghdad, or wherever. What are they supposed to do when they find somebody snooping around inside their systems?

Well, first of all, they should be responsible enough to provide adequate security from the start. But once they find out that it's some harmless kid […] I think the appropriate response would be perhaps to take my computers away like they did, and leave it at that. They could tell me that I can't use the internet for a while, to teach me a lesson, teach me that they actually do care about what I'm doing, and that I shouldn't do it again. But they shouldn't put the youth of America in jail.

Q: How does the prospect of sitting in jail for six months affect you?
R: First of all – six months. While it's not as long as some other sentences, it's still a long time. And that's six months of me being surrounded by people that did these actual crimes, did bad things to other people, to humanity. And I'm surrounding myself with these people that are lower than myself. Not to sound arrogant, but they lack morals, and it would be degrading to my character [...] and I'm worried.

Q: Are you trying to tell me that you don't think the crime you committed is on the same order? [...]
R: Not at all. This is just harmless exploration. It's not a violent act or a destructive act. It's nothing.

Q: They say that, at one point, you took possession of $1.7 million worth of software, and that you made them shut down and spend weeks with 13 or 14 important government computers down. That sounds serious.
R: Well, I think the price of the software is irrelevant, because the government overpays for everything. But it was source code that wouldn't even compile. The computer people know what I'm talking about. It was source code that wouldn't even compile without the proper equipment, or maybe it was just bad coding, I don't know. But the only reason I downloaded it was for the sake of learning what it is that they're doing, how they program, their techniques.

Q: And you learned basically that it was no good?
R: Yes. They did stupid, stupid things that an experienced programmer would know not to do. But as for claiming that the addition of computer security is damages? That demonstrates a serious lack of responsibility on the government's behalf. The failure to put adequate security up from the start, from as soon as they turn the computers on, is a lack of responsibility. And then they cover up their mistakes. They call it damages when a computer enthusiast such as myself demonstrates their ineptitude.

Q: What did that teach you about the state of computer security, and about the ability of public authorities and government people to police the security of the computer systems out there?
R: I certainly learned that there's a serious lack of computer security. If there's a will, there's a way, and if a computer enthusiast such as myself was determined to get into anywhere, be it the Pentagon or Microsoft, it's been demonstrated that it's possible and they will do it. And there's next to nothing they can do about it, because there's people with skill out there, and they'll get what they want.

Q: How would you assess the skill levels of the law enforcement people who eventually came knocking at your door?

R: Okay, they got lucky, because I didn't take any measures whatsoever to hide myself. I didn't cover my tracks at all, and had I done that, they would not have been able to catch me. If I wanted to, I could have hidden myself, but I didn't think I was doing anything wrong, so, why bother?

Q:You could have escaped detection?
R: I could have.

Q:You could have done a lot of damage?
R: If one was so inclined, you could have deleted files, or put a virus up or sell information to foreigners. You could perform a denial of service attack and cause the computers to stop performing. Someone could do any number of things that I did not do.

Q:Could you have done those things?
R: I could have.

Q:They couldn't have stopped you? And they couldn't have caught you?
R: No. They could not have caught me.

Q: What are you going to do now? People of my generation would ask if you've learned your lesson.
R: I've learned my lesson. I shouldn't do stuff like that.

Q:But it seems to me that the big lesson is just how vulnerable everybody is to this technology.
R: It's a lesson to us all.

Q: What are you going to do about it? Are you going to try and fix it?
R: Yes, maybe I'll start a computer security company.[19]"

From the U.S. Department of Justice

"Juvenile computer hacker sentenced to six months in detention facility –
Case marks first time a juvenile hacker sentenced to serve time
The Justice Department announced today that a 16-year-old from Miami has pleaded guilty and been sentenced to six months in a detention facility for two acts of juvenile delinquency. Under adult statutes, those acts would have been violations of federal wiretap and computer abuse laws for intercepting electronic communications on military computer networks and for illegally obtaining information from NASA computer networks. […] The juvenile, whose is known on the Internet as "c0mrade," admitted today in U.S. District Court in Miami that he was responsible for computer intrusions from August 23, 1999, to October 27, 1999, into a military computer network used by the Defense Threat Reduction Agency

[19] http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html

(DTRA). DTRA is an agency of the Department of Defense charged with reducing the threat to the U.S. and its allies from nuclear, biological, chemical, conventional and special weapons. In pleading guilty, "c0mrade" also admitted that he gained unauthorized access to a computer server, known as a "router," located in Dulles, Va., and installed a concealed means of access or "backdoor" on the server. The program intercepted more than 3,300 electronic messages to and from DTRA staff. It also intercepted at least 19 user names and passwords of computer accounts of DTRA employees, including at least 10 user names and passwords on military computers. In addition to the computer intrusions at DOD, on June 29 and 30, 1999, "c0mrade" illegally accessed a total of 13 NASA computers located at the Marshall Space Flight Center, Huntsville, Ala., using two different ISPs to originate the attacks. As part of his unauthorized access, he obtained and downloaded proprietary software from NASA valued at approximately $1.7 million. The software supported the International Space Station's (ISS) physical environment, including control of the temperature and humidity within the living space.

As a result of the intrusions and data theft, the NASA computer systems were shut down for 21 days in July 1999. This shutdown resulted in a delivery delay of program software costing NASA approximately $41,000 in contractor labor and computer equipment replacement costs. In addition to serving six months in a detention facility, as conditions of his guilty plea, "c0mrade" will write letters of apology to the Department of Defense and NASA and has agreed to the public disclosure of information about the case.[20]"

A famous example of black hat and white hat hackers

[…] On February 15, 1995 "Officials apprehended a computer criminal in North Carolina who allegedly broke into a computer at the San Diego Supercomputer Center (SDSC) in December and stole several software tools under development. A spokesperson for SDSC told HPCwire that the individual's arrest is the result of a collaboration among Federal agencies and computer security specialists at SDSC, including *Tsutomu Shimomura*, a well-known *security expert*. Shimomura has been working with Federal agencies to capture the criminal since December 25, when Shimomura found that an intruder had broken into his computer over the network, stolen several security tools under development, and deleted files in an attempt to hide activities. […]

Tools developed for network security, like those developed by SDSC researchers, may be similar to those developed by computer criminals – but criminals are using them to disrupt communication and destroy or alter the work of a nation. […] a report by Stephen Dill for the Associated Press includes comments by one official that described the alleged perpetrator, *Kevin D. Mitnick*, as *"the most wanted hacker in the world, a notorious computer vandal and a fugitive."*

[20] http://www.justice.gov/opa/pr/2000/September/555crm.htm, 21 September 2000.

> […] in more than two years on the run, Mitnick allegedly pilfered thousands of data files and at least 20,000 credit card numbers, worming his way into even the most sophisticated systems. He once broke into a top-secret military defense system as a teen-age prank, and apparently infiltrated one computer too many this time. One of his latest victims, computer security expert Tsutomu Shimomura, was so angered that he made it his crusade to track Mitnick down. […]
>
> Mitnick, 31, was charged with computer fraud, punishable by 20 years in prison, and illegal use of a telephone access device, which carries a maximum 15-year sentence. Both crimes are also punishable by $250,000 fines. He already was wanted in California for allegedly violating probation on a previous hacking conviction. A hearing was scheduled for Friday. […] Mitnick had been on the run since 1992. Authorities say he broke into many of the nation's telephone networks, and most recently he had become a suspect in a rash of break-ins on the global Internet computer network, Dill reported. […] Authorities characterize Mitnick as a program pirate obsessed with cracking secret access codes. He began hacking in high school, breaking into the school district's main computers and calling himself "Condor," from the Robert Redford CIA movie "Three Days of the Condor."
>
> As a teen-age prank in 1982, he allegedly broke into a North American Air Defense Command computer in Colorado Springs, Colo. He once altered a phone program to misdirect federal agents trying to trace his call, sending them barging into the home of a Middle Eastern immigrant watching television.
>
> In 1989, he admitted infiltrating Digital Equipment Corp.'s computer system and also stealing 16 MCI telephone codes. He was sentenced to a year in federal prison, where officials considered him so dangerous they wouldn't let him near a telephone, said Dill. After his prison term, Mitnick was under conditional release for three years. Authorities were chasing him for reportedly violating that probation when he disappeared in November 1992.[21]

From the U.S. Department of Justice

> Kevin Mitnick, who pleaded guilty to a series of federal offenses related to a 2½-year computer hacking spree, was sentenced today to 46 months in federal prison, United States Attorney Alejandro N. Mayorkas announced.
>
> Mitnick, 37, pleaded guilty in March to four counts of wire fraud, two counts of computer fraud and one count of illegally intercepting a wire communication. Mitnick's prolific and damaging hacking career, which made him the most wanted computer criminal in United States history, was ended when he was arrested in North Carolina in February 1995.
>
> In a global plea agreement filed in United States District Court in Los Angeles, Mitnick admitted that he broke into a number of computer systems and stole proprietary software belonging to Motorola, Novell, Fujitsu, Sun Microsystems and

[21] http://www.takedown.com/coverage/sdsc-experts.html, 16 February 1995

> other companies. Mitnick admitted using a number of tools to commit his crimes, including "social engineering," cloned cellular telephones, "sniffer" programs placed on victims' computer systems and hacker software programs.
> As part of his scheme, Mitnick acknowledged altering computer systems belonging to the University of Southern California and using these computers to store programs that he had misappropriated. He also admitted that he stole E-mails, monitored computer systems and impersonated employees of victim companies, including Nokia Mobile Phones, Ltd., in his attempt to secure software that was being developed by those companies. […] Once he is released from prison, Mitnick will be on supervised release for three years, during which time his access to computers and his employment in the computer industry will be severely restricted. […] The sentencing today brings to a close an investigation that started in 1992 when Mitnick, then a fugitive, commenced an unprecedented series of computer intrusions and electronic thefts from technology companies throughout the United States and the world. His combined sentence of 68 months incarceration is the longest sentence given to any computer hacker. If Mitnick violates the terms of his supervised release after he is released from prison, he could be sent back to prison for additional time[22].

Currently, K. Mitnick runs a security consulting firm and has authored several books.[23]

Unusual Chinese hackers

> *Chinese hackers pledge to reject cybercrime*
> Gong Wei and Wan Tao ask their peers to commit to a code on hacking standards. Two prominent Chinese hackers have released a convention calling for the rejection of cybercrime and are asking their peers to support it, as China is increasingly seen as the source of international hacking attacks and cybertheft. The two hackers, Gong Wei and Wan Tao, released their "Hackers' Self-Discipline Convention" to the Chinese media and posted its contents on the internet. The hackers declined to offer further comment, but the document presents itself as a moral code that

[22] http://www.justice.gov/criminal/cybercrime/mitnick.htm, 9 August 1999.

[23] "Mitnick Security Consulting, LLC, is a full-service information security consulting firm. Founded by Kevin Mitnick, Mitnick Security Consulting offers a comprehensive range of services to help businesses protect their valuable assets" (http://mitnicksecurity.com/). On his Facebook account K. D. Mitnick wears a Tshirt: "I am not a hacker, I am a security professional" (http://www.facebook.com/pages/Kevin-D-Mitnick/106309966073790).
Some Kevin. D. Mitnick's books:
"Ghost in the Wires: My Adventures as the World's Most Wanted Hacker" (2011)
"The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers" (2005)
"The Art of Deception: Controlling the Human Element of Security" (2003)

outlines appropriate hacking activities and eschews cybercrime. The document states that hackers will not obtain money through stealing from the public. Hacking groups will also not spread knowledge or tools that are meant to take income. "The public's privacy, especially that of children and minors, will be protected," the document says. Any activity to buy or sell people's private information is considered inappropriate[…][24]

7.6 Summary

The criminals who use the Internet to carry out and optimise their activities are cybercriminals. Information and communications technologies are the means and the targets of their criminality. They have integrated these technologies into their strategies to get rich, launder money, obtain power, or destabilize others. For them, the Internet is a tool to be used for many kinds of frauds, transactions, and general crimes. Whether it falls into the category of organised crime, gang crime, the activities of individuals or the result of simple delinquency, and regardless of whether the authors are qualified professionals or simply using the knowledge of others, a crime is a crime and has an impact on its victims. Even if the target of the crime is a computer or the data stored on one, these physical or virtual assets belong to someone or some organisation. Every offence or crime that is so recognised by the law causes damage and costs borne by both the victim and the wider public.

Similar to drug trafficking or economic crime, where the criminals rely on the chemists or the accountants who are the experts in the field, cybercriminals need the knowledge of IT specialists, and above all experts in system and network security. They have thus learned to "recruit" them and benefit from their skills. Still in analogy with traditional criminality, the real leaders rarely have dirty hands themselves, while it is intermediaries and small-scale players who are used and are vulnerable to reprisals and to the workings of justice.

These days it is common to use the word "hacker" to describe people capable of breaking or circumventing the security of systems and software or of exploiting their weaknesses – the idea of the black hat hacker. At the same time, IT security professionals operate in an entirely legal framework, and if their knowledge and tools are similar to those of the black hats, they can be described as white hat hackers. Certain commercial businesses in the field of information security have appropriated the word "hacking" in the phrase "ethical hacking" in order to sell security services based around performing

[24] http://www.computerworlduk.com/news/security/3304319/chinese-hackers-pledge-to-reject-cybercrime/, 19 September 2011.

penetration tests on systems. These very businesses can occasionally find themselves relying not only on white hats but also on black hats.

Those involved in cybercriminality are a numerous and heterogeneous group with differing motivations and backgrounds. It would be reductive to try to define a definitive typology of cybercriminals, as such an attempt would be unable to correctly reflect the diversity and complexity of all the participants.

Although it is not easy to know the motivations of cybercriminals, one way to differentiate them is to consider whether or not they have used their illegal activities for financial gain. This allows us to separate the professionals from the others, whom we have described as amateurs. In this latter category we find a wide range of individuals, from the very youngest to the most senior. Some of them may not really understand the significance of what they are doing or their ability to cause problems. Others, on the other hand, do these things deliberately.

They might have a feeling of superiority caused by a level of mastery of how the Internet works – a level certainly superior to that of the majority of Internet users and that of people who use out-of-the-book malware; this is fairly typical of hackers who want to show that they are better than the others.

Or in addition, they might have a feeling that hacking activities – hacktivism – are legitimised by their passion for the subject and by the very existence of the Internet, and that these activities are in some way imposed upon the hacker as natural outlets, with the subtext that the hacker is the holder of the ultimate truth and that these activities represent, in some way, a divine mission. Without greater knowledge of the precise circumstances, it is difficult to tell, when considering a person hidden behind a remote screen who uses multiple intermediary technologies and false identities (stolen identities, false identities, anonymised identities), whether the actions undertaken are driven by genuine feelings of citizenship, fanaticism, mysticism, or terrorism.

7.7 Exercices

1. What are the main motivations of cybercriminals?

2. What were the main motivations of *hackers* at the beginning of the Internet? How are these different from the current widely accepted use of the term *hacker*?

3. Are those involved in social engineering primarily IT engineers or criminals?

4. What is covered by the term *ethical hacking*? To what extent is this term an abuse of language? What would be a more appropriate term for this kind of activity?

5. What means are employed by criminals to avoid being identified and held responsible for illegal acts committed across the Internet?

6. What is meant by the term *cracker*? Is it a synonym for *hacker*?

7. How are *script kiddies* and *hackers* usually distinguished?

8. Are people who harass others over the Internet cybercriminals?

9. Suggest criteria for distinguishing types of cybercriminals and a possible means of classification.

10. Why do certain companies refuse to employ people who are, or who have been, *black hat hackers*?

Chapter 8

The Cybercriminal's Toolkits

8.1 Understanding the context

As demonstrated in previous chapters, the concept of hacking covers a wide range of activities associated with accessing computer resources belonging to a third party without authorisation.

All offensive uses of ICT in order to harm, degrade, inhibit, disrupt, deny, or destroy ICT resources are classified as cyberattacks. Cyberattacks are computer-driven attacks committed through cyberspace against targeted systems.

The impact of a cyberattack depends on its target and on how it functions. The impact can vary infinitely as a result of the precise nature of the target and the abilities and the motivations of the cybercriminals. Some attacks consist of hijacking or deceiving systems or means of security, or even breaking them, while others consist of the misuse of technologies. This is the case with, for example, denial of service attacks.

There are many ways of manipulating the possibilities offered by the suite of Internet protocols in order to exploit the weaknesses and vulnerabilities of ICT environments, to deceive the users and owners of systems to which the offender does not have legitimate access rights, and thereby to gain illicit access. The ingenuity of attackers is virtually limitless and, in general, they know how to change their approaches and exploit efficiently both the resources available and the vulnerabilities present. Attackers are increasing their knowledge, and their approaches evolve dynamically and permanently in order to exploit any new opportunities offered by the changing environment. Although it would be impossible to present an exhaustive list of the types and methodologies of attack, as these are numerous and undergo constant evolution, it is possible to identify certain constant factors. Some of these general principles are presented below.[1] Of course, this is not an attempt to present an exhaustive list of all the tools that are available in the marketplace, but rather an overview of the methods that cybercriminals employ and the weapons at their disposal.

8.2 Fundamental principles and constant factors of cyberattacks

Active and Passive Attacks

The different types of attacks can essentially be classified in two main categories: passive or active attacks (Figure 8.1). The methods of attack that modify data are described as *active* while those that rely on simple listening – the interception of data without altering them – are described as *passive.*

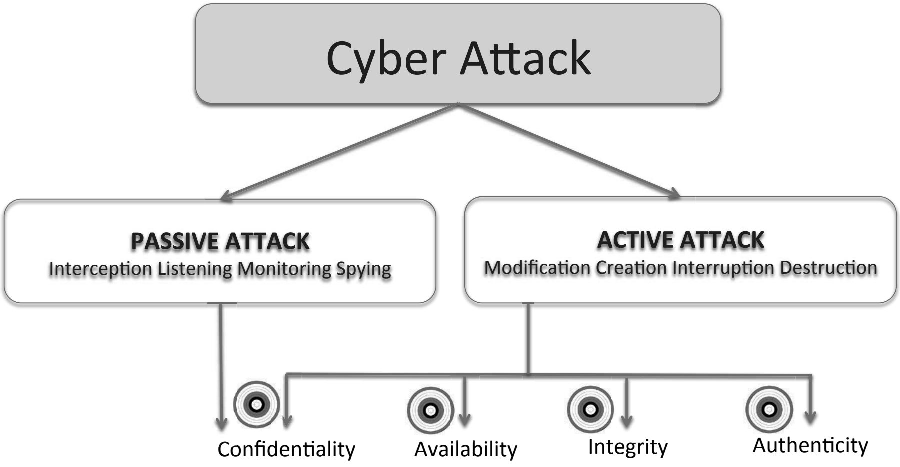


Figure 8.1 Active and passive cyberattacks.

[1] This chapter is not an instruction manual for performing cyberattacks, nor should it be read as incitement or encouragement to perform such attacks.

Cyberattack methodologies

Figure 8.2 shows the different phases of a cyberattack. The object of the first phase is to gather information and explore the potential vulnerabilities of an ICT system and gain the maximum information for future use. This phase can include studying the mechanisms and levels of security used for identification, authentication, access control, encryption, and surveillance, and then identifying technical, organizational and human weaknesses in the environment. The attacker often attempts to coax naïve or credulous users into revealing information that can be used to design an attack (this is called social engineering[2]). In fact, the ideal situation for the attacker is to acquire the access credentials of legitimate users that can then be used to access the systems and perform various operations such as reading or modifying data. *Social engineering* refers to techniques, procedures, and measures used by malicious people, who usually take advantage of the users' credulity to obtain, *inter alia,* their passwords and connection parameters and usurp their digital identity, thereby breaching the system's security by pretending to be authorized visitors. The aim of social engineering is to find and exploit human vulnerability in order to manipulate a person. The victim can be conducted to act against his or her own interest but in a way beneficial to the social engineer. Social engineering is often seen as "the art of manipulating people." It mainly constitutes the first step of phishing actions or of targeted cyber attacks. (Figure 8.3).

Hackers can also look for and exploit known – but not yet repaired (patched) – *security vulnerabilities*, often using means such as attack libraries and attack toolkits that are widely available online to penetrate systems (phase 2). The attacker will usually configure these tools to correspond to certain requirements or manufacture a new specific tool from the elements that are already available in order to access the target system and perform malicious operations (phases 3 and 4).

There then follows a *retreat phase* (phase 5) that is intended to cover up the traces of the attack, at least in the short-term, or to ensure that any traces do not allow the hacker to be identified or localized. Hackers increase their anonymity by using aliases, usurping legitimate users' identities, or covering their tracks by means of multiple intermediate (relay) systems. The objective of the careful attacker is to avoid leaving traces of the visit to targeted systems. The attacker has a clear motivation to delete any traces that could lead to identification and localisation, given the severe penalties for illegal activities

[2] Social engineering is the manipulation of someone in order to persuade him or her to provide confidential information.

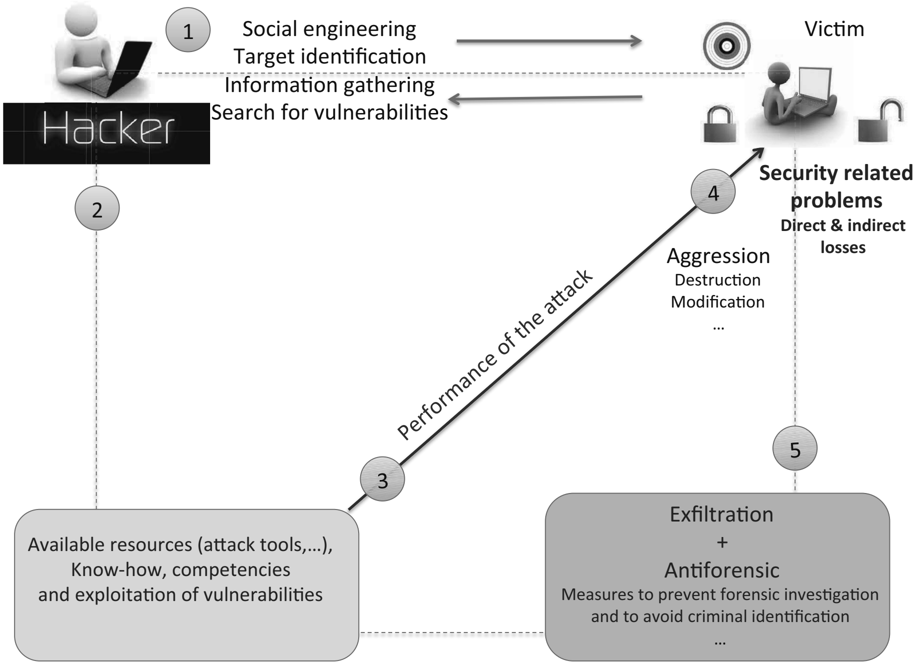

1
Social engineering
Target identification
Information gathering
Search for vulnerabilities
Victim
Hacker
2
Security related problems
Direct & indirect losses
4
Aggression
Destruction
Modification
...
Performance of the attack
3
5
Available resources (attack tools,...),
Know-how, competencies
and exploitation of vulnerabilities
Exfiltration
+
Antiforensic
Measures to prevent forensic investigation
and to avoid criminal identification
...

Figure 8.2 Main characteristic phases of a cyberattack

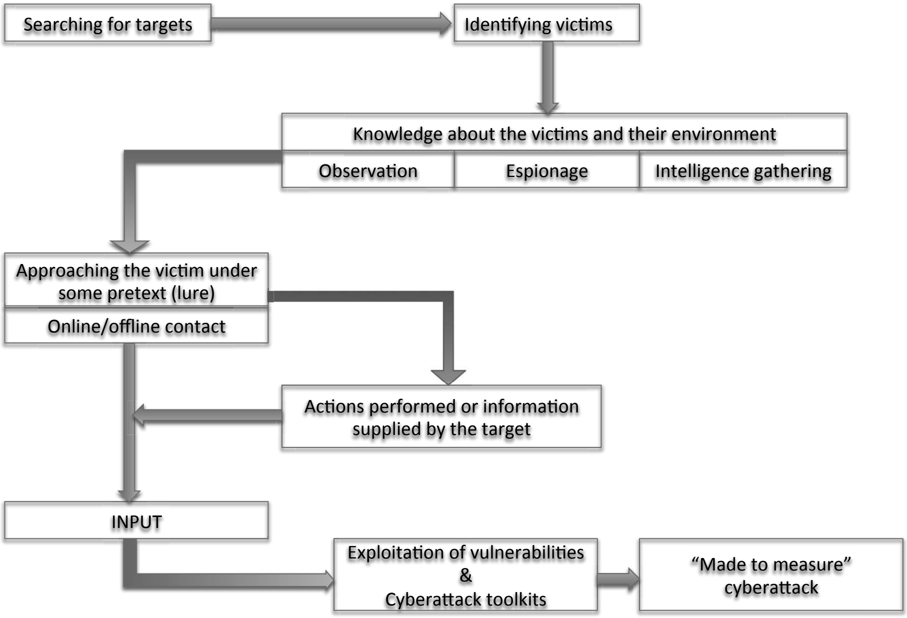

Searching for targets
Identifying victims
Knowledge about the victims and their environment
Observation
Espionage
Intelligence gathering
Approaching the victim under some pretext (lure)
Online/offline contact
Actions performed or information supplied by the target
INPUT
Exploitation of vulnerabilities & Cyberattack toolkits
"Made to measure" cyberattack

Figure 8.3 The social engineering cycle and social intelligence.

in certain contexts and jurisdictions. An attacker can also intentionally modify digital traces to mislead any audit or security mechanisms, computer forensics software, and specialists.

Generally speaking, the necessary conditions for a successful attack are:

- knowledge of the target system (function, service, configuration, security policy and tools, administration);
- efficient use of programs (called *exploits*) that automatically exploit vulnerabilities to break into a computer;
- capacity of the aggressor to cover his tracks to avoid being detected and identified;
- rapidity of the attack (the attack is so fast that reactive security measures are ineffective).

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

An attack can target a security system (firewall, authentication server, etc.), a security-related system (router, DNS, etc.), or a system that has no link to security measures, services or functions, such as workstations or web servers (Figure 8.4). According to the type of system targeted, the attack will be more or less difficult to carry out, and more or less rapidly detected, with a varying degree of negative impact.

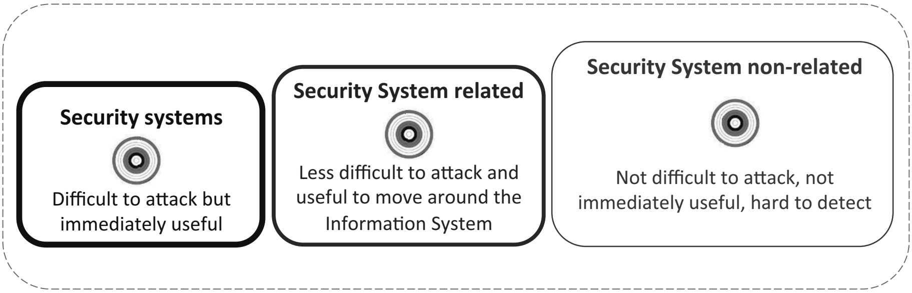

Security systems
Difficult to attack but immediately useful
Security System related
Less difficult to attack and useful to move around the Information System
Security System non-related
Not difficult to attack, not immediately useful, hard to detect

Figure 8.4 Targeted systems and levels of cyberattacks.

In each case the hacker exploits the weaknesses of the target system. Given that computer systems are complex by nature, they are always vulnerable; even dedicated security systems can be both vulnerable and fallible. Some systems are easy to attack; others are much less so. Using a methodical approach to perform an attack is one key element of success, while for the system owners, there is no method that guarantees full protection.

8.3 Spam and phishing: assets for criminals

Redirected from its original purpose as a tool for marketing, spam has become a means of distributing malicious software (malware and crimeware) and a mechanism for carrying out frauds. The sending of massive quantities of unsolicited electronic messages allows criminals to contact a huge number of Internet users. Previously, spam was regarded primarily as a nuisance, but nowadays spam represents a real threat. It decreases user productivity and has direct and indirect costs on people and organizations affected by it.

At its worst, spam resembles an e-mail bombing attack, with overloaded mail servers, full user mailboxes, and the irritation that this provokes.

Spam leads to the propagation of viruses, Trojans, spyware and phishing attempts, and to the infection of computers. In some cases, these systems can become zombie computers, part of botnets (robot networks) remotely controlled by a third party. They can be activated and able to launch waves of spam, begin phishing attempts, or to commit cyberattacks such as DoS attacks by flooding or infecting other systems.

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 8.5). In general, hackers conduct phishing attacks by using e-mail messages that are forged to

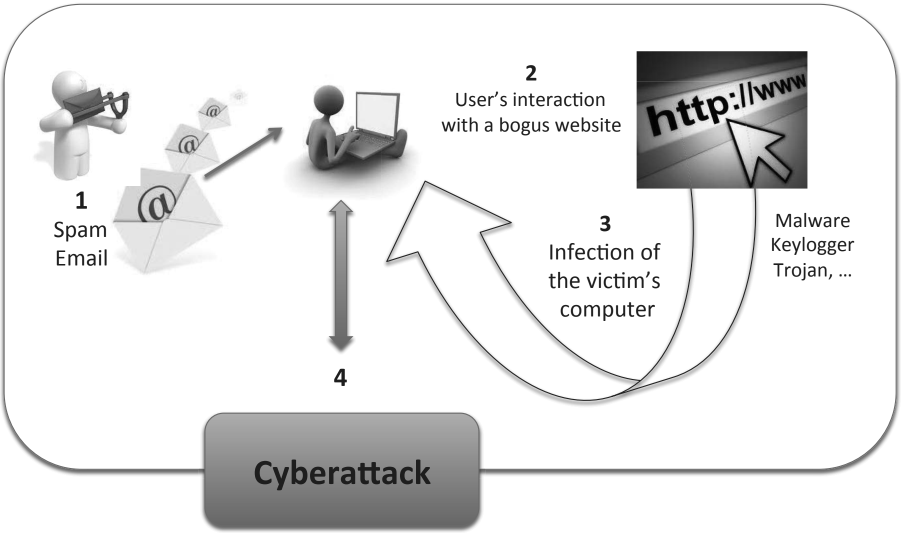


Figure 8.5 A phishing attack.

appear as though they come from a genuine institution with which the user may have dealings or have a commercial relationship (e.g. the post office, a bank, or an online service site). Attackers may also use a telephone call, instant messaging (IM) or cell phone text messages. They may even approach victims in person. The most common lure is an e-mail asking the user to update his account or change his password for security reasons.

Example – spoofed email

Customers of a bank receive a spoofed e-mail explaining that the bank is performing 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, all based on a scammed e-mail luring a bank's customers to a spoofed website.

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 colours of a company with which the user is very familiar. Phishers use botnets in order to simultaneously launch a large number of phishing attacks.

Example – Phishing

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 to enter 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.

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 his contact list. A victim is less likely to suspect an instant message from a friend than an e-mail from some organization he used to deal with.

Example from a real case

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.

Cybercriminals know that organizations and Internet service providers use anti-spam detection software and have taken preventive security measures, such as blocking some IP addresses. Those criminals keep making their own adjustments – they invent new methods to circumvent detection tools. A number of awareness campaigns driven by private businesses or public institutions now exist, as do associations such as the Anti-Phishing Working Group (APWG)[3], which is a global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that results from phishing, pharming and email spoofing of all types.

Spear phishing 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. Many attackers prefer this method to using fake websites or malware.

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.

[3] www.antiphishing.org/
The Anti-Phishing Working Group has more than 2,500 members who represent 1,600 companies and agencies worldwide (banks, Internet Service Providers, hundreds of technology vendors, and national and provincial law enforcement agencies).

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 a 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 that 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 that contains malicious content. This malware is mostly comprised of:

- Trojans or keyloggers that gather credentials by recording keystrokes;
- screenloggers that monitor screenshots from the computer;
- 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 web browser and redirect HTTP traffic to illegitimate sites.

Malware can also be used to manipulate:

- the host files that are used to maintain the mapping between DNS addresses and IP addresses;
- 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 a 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. Figure 8.6 summarizes the different kind of phishing attacks.

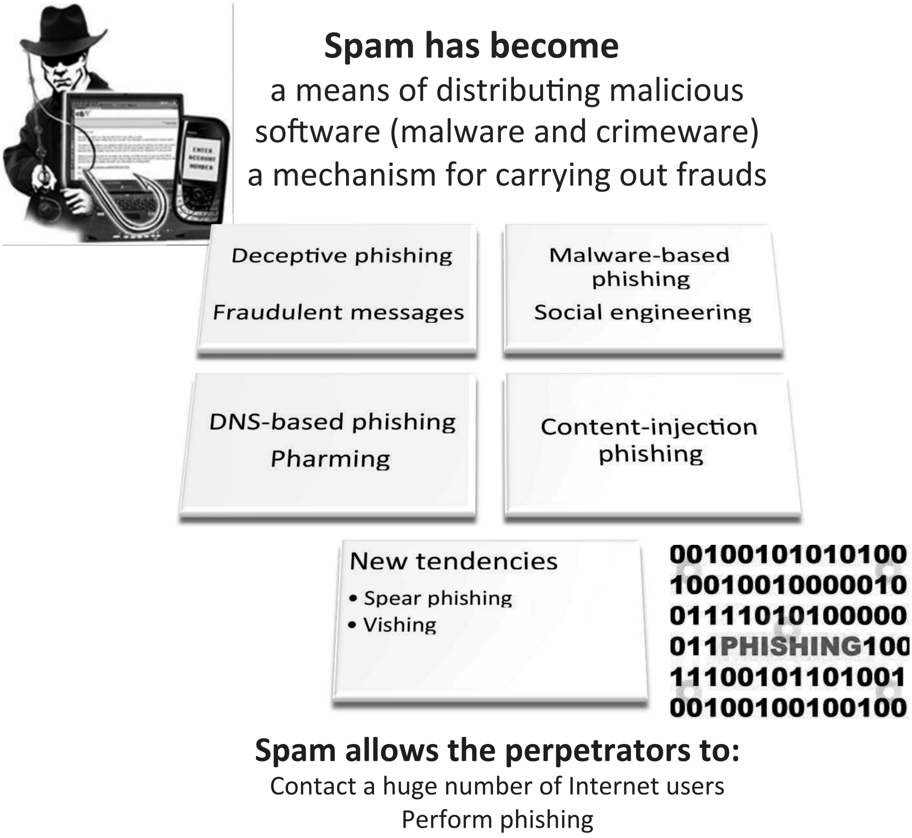


Figure 8.6 A summary of the different kinds of phishing attacks.

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 known as *zombies*. 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 by a Trojan, through e-mails, or via a malicious website. Bots also propagate by mass scanning to find vulnerabilities in services. The hacker perpetrates the infection and the attack without the user's knowledge. As mentioned above, the hacker can run thousands of bot computers to launch DoS attacks. He can attack such targets as an e-commerce organization which allows on-line payments and money transfers, or online auction companies.

Bots never work alone. They are part of a big network of infected computers called a *botnet*, a 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 control the zombies from a distance and to launch coordinated and simultaneous attacks. The geographical location of the zombie machines stretches around the globe.

Cybercriminals control bots through communication channels. The most common control channel is IRC, firstly because it is a popular protocol well adapted to run on different machines in a distributed way; and secondly 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 does make the bot system 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 now often use new communication methods such as 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 disconnection, 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 have been using web-based controllers, such as the HTTP protocol, to control botnets and instant message controllers. VoIP can be a new and powerful communication channel for attackers, because almost all applications are proprietary and use encryption for the travelling data. VoIP applications seem to be a better way for attackers to control their zombies, erase their tracks and cover up their attacks.

Bots have a central role in the cybercriminal world. Botnet owners either launch attacks themselves, or they rent their network of zombie computers to any third party who wants to launch an attack. Bot networks are thus a real threat to all Internet-connected systems. Various attacks can be performed by cybercriminals using bots and botnets, such as:

- drowning websites and 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;
- advance fee fraud;
- extortion, by threatening organizations with a DDoS 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;

The primary reason for using botnets is the potential to launch large-scale DDoS attacks. An attacker has at his disposal thousands of zombie computers ready to simultaneously launch an attack on one or several targets. The attack will choke the bandwidth of the server, which will cause the service to be unavailable. This often forces e-commerce companies to cease their activities temporarily. 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.

8.4 Means of obtaining connection parameters to access systems

Hackers 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 presented here after and summarized in Figure 8.7.

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 might just as well give out the password to the wrong person.

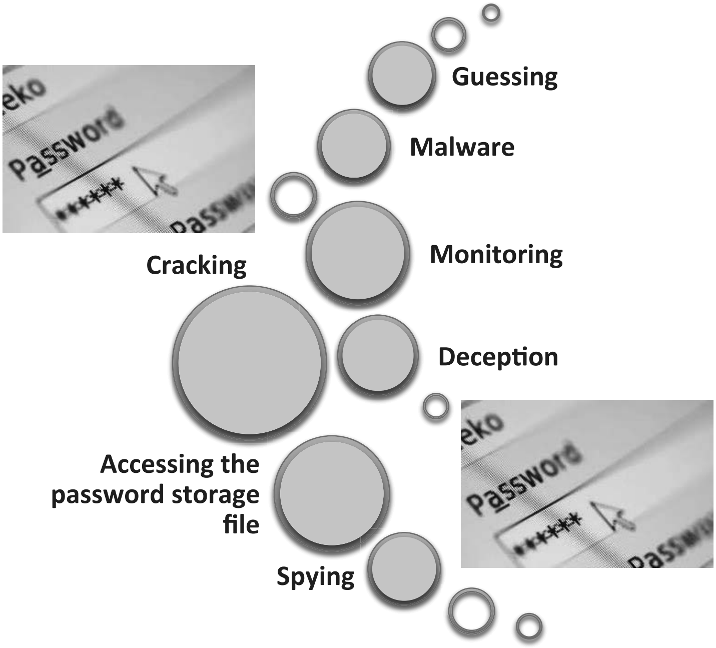


Figure 8.7 Tricks and methods to gain access illegally to computers.

Deception: The attacker poses 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 contact the user by telephone or by electronic messaging. Some malevolent individuals are not computer geniuses, but simply crooks who maliciously obtain keys corresponding to the system locks they want to open.

This can be done by both phishing and social engineering methods. Phishing is a kind of gathering technique to obtain personal or secret data from users by a confidence trick. Nowadays, social engineering is facilitated by data left on social networks that are easily accessible and used to target people very precisely and efficiently. Sophisticated phishing message (known as spear phishing, above) with credible motives will be more accurate and can incite even smart people to provide confidential data or perform specific actions such as connecting to a website, downloading a document, or executing a file that contains a malware. Spam (including spam over Internet telephony) and hijacked e-mail accounts contribute to the performance of phishing.

Listening to traffic: The attacker intercepts or listens to unencrypted data transmitted over the network through communications protocols (sniffing, monitoring). If fraudsters cannot rely on complicity from inside the organization in order to obtain passwords directly, they can electronically intercept data from communications protocols or access files containing the passwords.

Software: A "Trojan horse" is installed on a user's workstation, where it clandestinely records the parameters used to connect to remote systems. Simple passive monitoring of IP packets is sufficient to capture passwords through communications protocols that transmit them without encryption. Such traffic analysis software is generally delivered as a standard with various operating systems, while other such software is often available as freeware. These tools operate on any PC by "sniffing" and analyzing the data in transit, and then extracting passwords that are transmitted unencrypted by the user during connection.

A *sniffer* is a passive entity that listens to and records the data that crosses it without modifying the data. For this reason, its presence in a network can be 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. When done carefully, this can result in the sniffer being effectively active only on one segment of the network. This type of security measure, which relates to the network architecture, is regarded as proactive, as it is designed to prevent problems from arising.

Usually network and system administrators use these tools and techniques for monitoring to manage 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.

Another variant consists of introducing a Trojan horse with a different purpose onto the user's workstation. This time a small program will substitute 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 stored by the Trojan horse, which then transmits it to a message server that the fraudster has already configured. In the meantime, the real user would not have been able to connect to his systems since the real login program had not been executed. The user would probably have seen an "incorrect password error" type message and would typically think that an error had been made in providing his credentials. He would then try to log in again, this time providing identification and a password, which would now be accepted by the real login program, granting access. Because such input errors and problems in logging in are so common, typically users would not notice anything out of the ordinary.

Accessing the password storage file: For an authentication system to function, all user passwords have to be stored somewhere on a machine. 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 to the file and apply decryption software – utilities are available, in particular on the Internet, for this purpose, although decryption is not necessarily a trivial operation and sometimes requires particular competencies.

Cracking passwords that are sent in encrypted form. The passive eavesdropping of data in transit can lead, after the use of captured passwords, to illicit system intrusions. One means of protection is to encrypt 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.

If the malevolent person knows which cipher algorithm is in use, he can 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, a so-called dictionary attack. By mass comparisons of intercepted passwords with dictionaries of encrypted passwords, a hacker can guess the password used.

Spying on users by activating their multimedia peripherals to record their connection parameters. Personal computers sometimes have an integrated video camera and microphone that can be used to monitor the user's behaviour and spy on him. This can allow hackers to capture confidential information, such as passwords, used to access protected systems. Therefore, it is advisable for vigilant users to:

- systematically turn off these peripherals when it is not explicitly necessary to use them;
- or use peripherals that alert the user – by a coloured light, for example – when they are active.

Whatever the mode of interception of the passwords, the users are unaware that their access parameters have been recorded by entities not entitled to do so. This is a threat for organizations as well as for individuals. The former may accuse the latter of being responsible for malicious incidents that were, in fact, carried out by someone else who had usurped the user's identity.

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

From the FBI

> *Former Security Guard Who Hacked Into Hospital's Computer System Sentenced to 110 Months in Federal Prison*
>
> […] In May 2010, McGraw, a/k/a "Ghost Exodus," 26, of Arlington, Texas, pleaded guilty without a plea agreement to an indictment charging two counts of transmitting a malicious code. He has been in custody since his arrest in June 2009. During his 11:00 p.m. to 7:00 a.m. shift at the North Central Medical Plaza, McGraw gained physical access to more than 14 computers, including a nurses' station computer on the fifth floor and a heating, ventilation, and air conditioning (HVAC) computer located in a locked room. The nurses' station computer was used to track a patient's progress through the Carrell Memorial Clinic and medical staff also used it to reference patients' personal identifiers, billing records, and medical history. The HVAC computer was used to control the heating, ventilation, and air conditioning for the first and second floors used by the North Central Surgery Center.
>
> McGraw installed or transmitted a program to the computers that he accessed that allowed him, or anyone with his account name and password, to remotely access the computers. He also impaired the integrity of some of the computer systems by removing security features, e.g., uninstalling anti-virus programs, which made the computer systems and related network more vulnerable to attack. He also installed malicious codes (sometimes called "bots") on most of the computers. Bots are usually associated with theft of data from the compromised computer, using the compromised computer in denial of service attacks (DDoS), and using the computer to send spam. McGraw knew his actions would damage the security and integrity of the computers and computer systems. McGraw was the self-proclaimed leader of a hacking organization called the "Electronik Tribulation Army" (ETA). He advocated compromising computers and computer systems in instructions that he posted online for members of the ETA and other individuals interested in engaging in computer frauds and participating in DDoS attacks.
>
> In this case, McGraw admitted that he intended to use the bots and the compromised computers to launch DDoS attacks on the websites of rival hacker groups. ETA's rival hacker groups included "Anonymous," the hacker group currently claiming responsibility for attacks against PayPal and others in support of Wikileaks.
>
> On Feb.12, 2009, McGraw abused the trust placed in him and bypassed the physical security to the locked room containing the HVAC computer. At approximately 11:35 p.m., he began downloading a password recovery tool from a website, which he used to re-recover passwords. By Feb. 13, 2009, at approximately 1:19 a.m., McGraw, again without authorization, physically accessed the HVAC computer

and inserted a removable storage device and executed a program which allowed him to emulate a CD/DVD device. He remotely accessed the HVAC computer five times on April 13-14, 2009.

On April 28, 2009, at about 1:45 a.m., McGraw abused the trust placed in him as a security guard and accessed without authorization a nurses' station computer. McGraw made a video and audio recording of what he called his "botnet infiltration." While the theme of "Mission Impossible" played, McGraw described step by step his conduct, accessing without authorization an office and a computer, inserting a CD containing the OphCrack program into the computer to bypass any passwords or security, and inserting a removable storage device into the computer which he claimed contained a malicious code or program. The FBI found the CD containing the OphCrack program in McGraw's house and found the source code for the bot on his laptop.

McGraw was aware that modifying the HVAC computer controls could affect the facility's temperature. By affecting the environmental controls of the facility, he could have affected the treatment and recovery of patients who were vulnerable to changes in the environment. In addition, he could have affected treatment regimes, including the efficacy of all temperature-sensitive drugs and supplies.

He was also aware that the nurses' station computer was used to access and review medical records. While he claims that he did not review or modify patient records, and the government is not aware of any evidence to the contrary, by gaining administrator access to these computers he would have had the ability to modify these records.[4]

8.5 Some basic attacks

Malware attacks

Malicious code is any program that can deliberately and unexpectedly interfere with the normal operation of a computer. Often malware programs are designed for financial gain but other motivations can include vandalism, mischief, or ideological positions. Malware is a category of malicious code that contains viruses, worms, or Trojans. The number of attacks continues to grow – and computer viruses have become veritable pandemics. They have become ubiquitous, affecting everyone in every sector of activity. No system, server, desktop, laptop or mobile phone is immune. No hardware or software platform is immune either.

The mechanisms used to propagate viruses from one system to another vary. SMTP (Simple Mail Transfer Protocol) is the main vector of propagation,

[4] http://www.fbi.gov/dallas/press-releases/2011/dl031811.htm; March 18, 2011.

due to the fact that e-mail delivery is the most commonly used application. Other vectors used to spread malicious codes are:

- peer-to-peer file-sharing networks;
- remotely exploitable vulnerabilities;
- IRC (Internet Relay Chat);
- 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 that contains a Trojan, can lead to infection by, and propagation of, the malware.

Malicious code can target computers and mobile devices. As smartphones contain a great deal of user-installable software, these represent new sources of vulnerability and, therefore, new opportunities to install programs that can have a negative impact on security. Malware includes the following kinds of software (Figure 8.8):

- downloaders, which are used to download and install data and programs remotely;
- keyloggers, which monitor 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 offensive computers. As mentioned above, they can be used for several kinds of malicious actions, such as spamming purposes, phishing attacks, intrusion attacks, or for the distribution of adware, for example;
- adware (advertising software), which is used to customize business transactions;
- spyware, which is used to clandestinely record information;
- viruses and related products, such as worms, Trojan horses, and logic bombs.

A virus consists of malicious code that is installed in a system without the user’s knowledge and has the capability of replicating itself. In the case of polymorphous viruses, the replication is not exact, but rather a mutation. Frequently viruses exploit security holes in operating system platforms, such as Windows. The computer will be 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. They can be present in material such as a CDs or USB devices if the production source was itself contaminated.

The purpose of a computer virus, like that of its biological counterpart, is to reproduce and propagate itself. It does so by moving from computer to computer, attaching copies of itself to programs and, most commonly, e-mails. This usually occurs in connection with some user action. The damage that viruses cause to the integrity of the contaminated information resources may range from mild annoyance to major destruction, with an impact on system availability, integrity and confidentiality. The main effects are loss of data, loss of working time, loss of public image, and loss of confidentiality.

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.

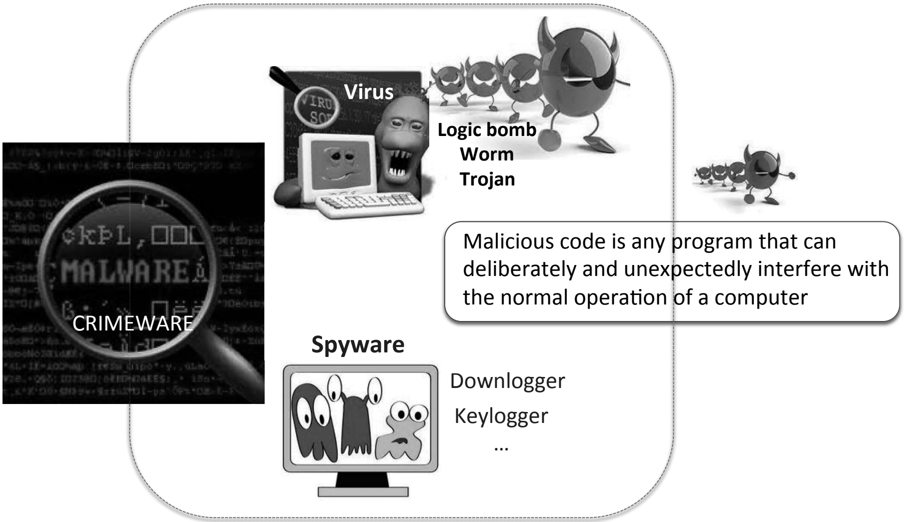

Virus
Logic bomb
Worm
Trojan
Malicious code is any program that can deliberately and unexpectedly interfere with the normal operation of a computer
MALWARE
CRIMEWARE
Spyware
Downlogger
Keylogger
...

Figure 8.8 Types of malware.

Example from a real case

A virus hits a country's 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 ignored. The investigation concludes 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 viruses have a direct effect, although 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. Viruses can be distinguished on the basis of their signature, behaviour, how they replicate and spread, or the types of malfunctions they induce.

Today, the principal objective associated with viruses is no longer gratuitous large-scale data destruction. Instead, they are usually designed to make money, as their inherent characteristics facilitate their use for fraud and have thus become highly lucrative tools for organized criminals engaged in financial crime.

The following are generic countermeasures to prevent virus infection and damage:

- resolve security holes (by systematically updating operating systems and applications);
- be familiar with current trends and reports of attacks;
- conduct virus scans regularly while updating the virus signatures of anti-virus software;
- maintain copies of boot media that will allow virus detection and removal from infected machines;
- do not open the attachments of suspicious e-mails;
- check the 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 has 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" or "Crazy Illegal sex." 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 or keystroke loggers. Instead, it may simply aim to destroy all important files on the computer. In order to accomplish this feat, the worm injects file deletion instructions onto servers.

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.

A 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 its capacity to mislead the user while appearing to be a useful program. Most often, malicious code is designed to steal banking information.

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 piece of software. In order to download it freely, the recipient has to click the provided URL, which redirects the user to a phishing website to run a Trojan horse.

Using an attack "toolkit" available on the Internet, offensive code can be installed on 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 (information gathering, activity 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.

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 such as "credit card," "account," or "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: carrying out surveillance, personal data theft, illicit uses of resources, perpetrating attacks, and disseminating and controlling tools used for DDoS attacks. Thousands of these programs are in circulation. Their objective is financial gain.

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.

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.

Crimeware is another word to describe malicious software designed to:

- perform illegal acts;
- steal personal information;
- automate crime.

Crimeware can include spyware, keystroke loggers, and bots. Most often crimeware gathers confidential information, such as passwords or credit card numbers, or 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 and confidentiality. It is mainly used for eeconomie crime identity theft, and personal profiling (Figure 8.9).

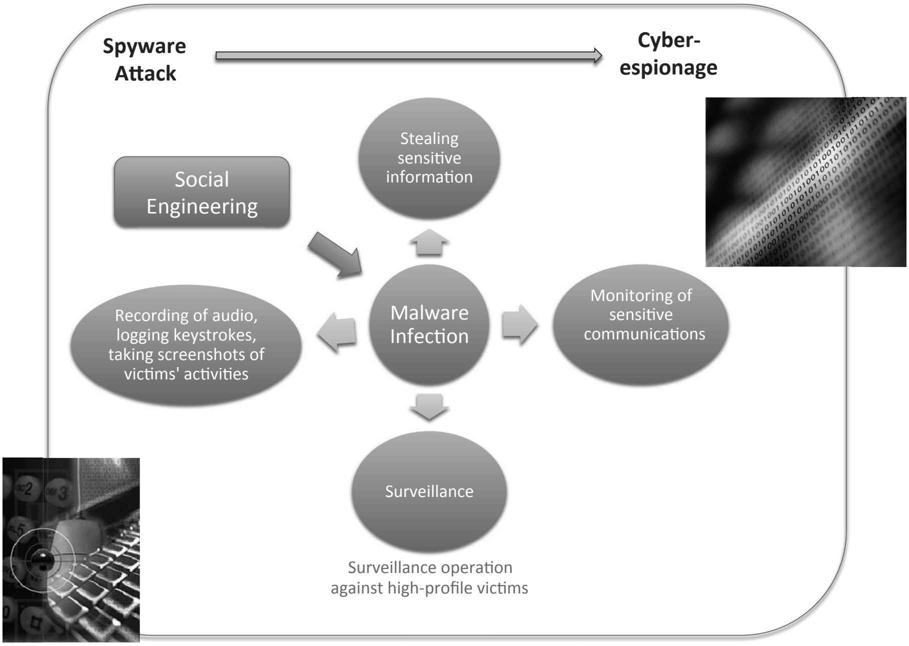

Spyware Attack
Cyber-espionage
Social Engineering
Stealing sensitive information
Malware Infection
Recording of audio, logging keystrokes, taking screenshots of victims' activities
Monitoring of sensitive communications
Surveillance
Surveillance operation against high-profile victims

Figure 8.9 Spyware attack.

Usually, hackers use spyware to gather personal information, such as identifiers, passwords, and bank account numbers, in order to impersonate bank customers.

Another effect of a spyware attack is to reduce computer system performance while spyware is working in the background and then is connecting to remote servers to upload the collected information. This can cause negative effects, such as the loss of network bandwidth, increased remote access costs, and network crashes. Furthermore, firewalls cannot intercept spyware programs, because the program is downloaded at the user's request, or accompanies antivirus software that is not malicious by nature.

Example

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 a significant black-market run on gaming farms.

Criminals can steal thousands of names and ID numbers from online gamers via malware hidden in malicious websites. This is called mass identity theft. Generally, a player needs to enter an 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.

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 hacker can potentially use stolen resident registration numbers to commit financial fraud and cause other damage.

Normally, spyware is bundled with another desirable program or downloaded from 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 behaviour and gathers information.

Spyware programs often include an End User License Agreement (EULA) as any legitimate application. 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 they do not know what to look out for, or they do not clearly comprehend the meaning.

Generally speaking, the best ways to overcome these problems are to educate users about these threats, and for an organization to define policy rules regarding the downloading of software. Far too often, users often do not recognize 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:

- it prevents the installation of spyware using real-time protection by scanning incoming data and disk files at the time they are downloaded;
- 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.

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. Submerged with far more requests than it can cope with, the system 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 communications.

Hackers 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 can cause serious malfunctioning that can eventually lead to system shutdown (Figure 8.10). A *distributed denial of service* (DDoS) attack is the term applied to an attack originating simultaneously from several different computers distributed over the Internet.

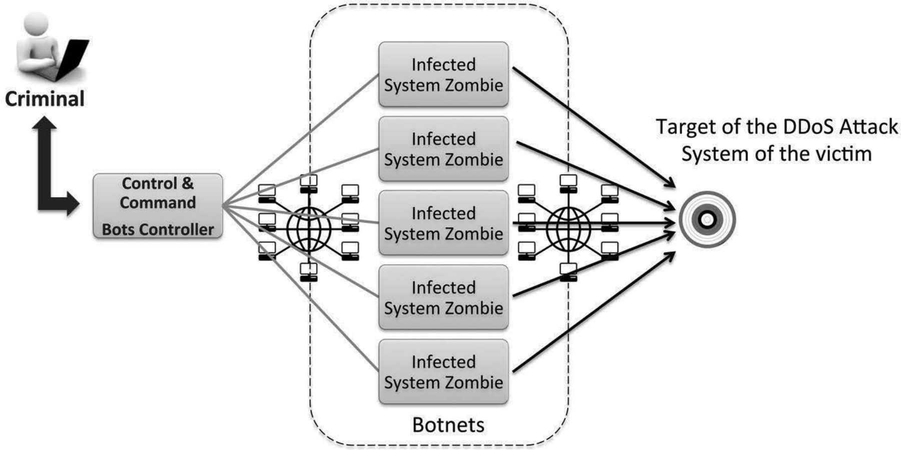


Figure 8.10 A distributed denial-of-service attack.

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, such 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 eighty other user identities and installed a password cracker tool directly on the server to find user passwords. This new attack caused more disruption of service, with significant financial consequences for the association.

There are three basic ways to attempt a DoS attack. These involve:

- the consumption of all resources, such as bandwidth, preventing legitimate traffic;
- the destruction or alteration of configuration information;
- 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 network connectivity in order to prevent hosts from communicating. For example, in a SYN 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, 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. The attacker sends a large amount of ICMP echo-requests (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.

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 breakdown of the network.

Organizations have 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, for example, could result in the overheating of some electronic devices and the disruption of a whole network.

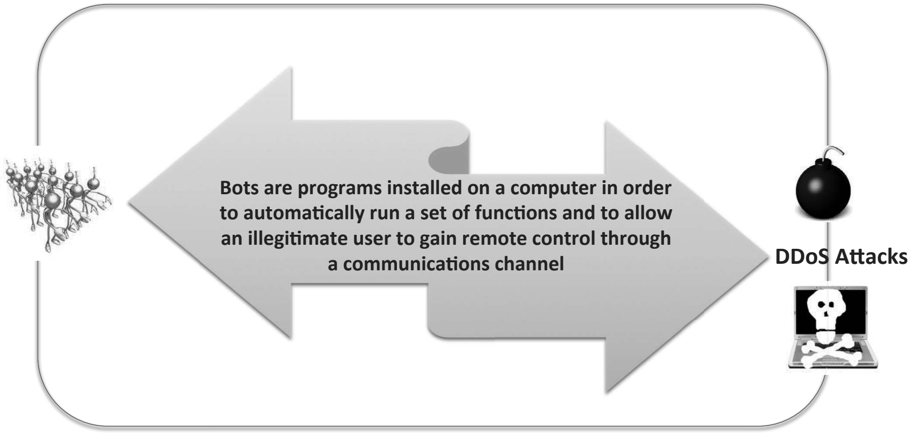

Bots are programs installed on a computer in order to automatically run a set of functions and to allow an illegitimate user to gain remote control through a communications channel
DDoS Attacks

Figure 8.11 Zombie computers and botnets for distributed denial of service attacks.

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. For example, zombie computers can bombard a system with thousands of e-mails, causing denial-of-service at the mail server – and thereby deny the service to legitimate users (Figure 8.11).

Example

A national police force caught a young boy and charged him with launching, for his own amusement, 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.

An effective way for hackers to increase the impact of their efforts and reduce their risk of identification is to create what is known as a *botnet*. Essentially, unsuspecting third parties have malicious software installed on their machines as result of coming into contact with malware, and this software is controlled and configured by the originator to perform a specific task, such as flooding a mail server with messages, flooding an authentication server with login requests, or bombarding a network device with ping requests. If the hacker can infect tens or hundreds of machines in this way, there will be a corresponding increase in the harm that can be done, without any need for increased resources in the form of computing power or bandwidth.

News from Reuters

> Websites of exchange operators Nasdaq and BATS have been attacked by hackers over the last 24 hours, causing ongoing disruptions for those trying to use the sites, spokespersons for the companies said on Tuesday.
>
> Only the banner carrying the logo at the top of the web page for www.nasdaq.com was visible during repeated attempts to access Nasdaq's site on Tuesday afternoon. Trading in Nasdaq-listed stocks has not been affected, however. A Nasdaq OMX Group spokesman confirmed that it had been suffering a denial-of-service attack (DOS) since late on Monday but said they had not located the origin of the attack and were unable to say when it would be resolved. Another site, www.nasdaqtrader.com, was also affected.[5]

From the FBI

> *Charges in Distributed Denial of Service Attack* Against Santa Cruz County Website – Defendants Alleged to Be Part of "People's Liberation Front," Hacking Group Associated with "Anonymous"[6]
>
> Today, *botnets are the weapon of choice of cyber criminals.* They seek to conceal their criminal activities by using third party computers as vehicles for their crimes. […]

[5] http://www.reuters.com/article/2012/02/14/us-nasdaq-attack-idUSTRE81D21720120214; 14 February 2012.

[6] http://www.fbi.gov/sanfrancisco/press-releases/2011/charges-in-distributed-denial-of-service-attack-against-santa-cruz-county-website; 22 September 2011.

> A botnet is a collection of compromised computers under the remote command and control of a criminal "botherder." A botherder can gain control of these computers by unleashing malicious software such as viruses, worms, or trojan horses. By executing a simple task such as opening an attachment, clicking on an advertisement, or providing personal information to a phishing site (a fraudulent site that mimics a legitimate site), an individual computer user has unintentionally allowed unauthorized access. Bot operators will then typically use these compromised computers as vehicles to facilitate other actions such as commit identity theft, launch denial of service attacks, and install keystroke loggers.[7]
>
> *Mafiaboy Pleads Guilty*
> The National Infrastructure Protection Center and the Federal Bureau of Investigation (FBI) announced today that on January 18, 2001, the 15-year-old male known on the Internet as Mafiaboy, appeared before the Montreal Youth Court in Canada and plead guilty to 56 counts. These counts include mischief to property in excess of $5000 against Internet sites including CNN.com, Yahoo.com, and EBay.com, in relation to the February 2000 Distributed Denial of Service (DDoS) attacks. In each of these instances, the DDoS attacks prevented the victim sites from offering their web services on the Internet to legitimate users. The other counts relate to unauthorized access to several other Internet sites, including U.S. universities.[8]

Mafiaboy was one of the first to launch the denial of service attacks against commercial websites in February 2000 that have since been highly publicized. He was identified while bragging about his exploits on the Internet – his arrest was possible only because of his boasting.

From Interpol

> The Police Service in the Maldives has arrested four individuals suspected of involvement with recent cyber attacks against the internet service provided by local telecom giant Dhiraagu. Police said the suspects arrested in the capital Male and Addu atoll included a 16-year-old, two 17-year-olds and a 28-year-old man. The three minors were reportedly caught red-handed with the equipment used for the denial of service attack, following an investigation by the Maldives Police Service with technical and operational assistance from INTERPOL's High Tech Crime Unit at the world police body's General Secretariat in Lyon.[9]

[7] http://www.fbi.gov/news/pressrel/press-releases/bot-roast-ii-nets-8-individuals; 29 November 2007.

[8] http://www.fbi.gov/news/pressrel/press-releases/mafiaboy-pleads-guilty; 18 January 2001.

[9] http://www.interpol.int/News-and-media/News-media-releases/2011/N20110117; 17 January 2011.

Defacement attacks

A defacement attack is carried out by replacing the victim's web page with a forgery, wherein the content of the forged page (e.g. pornographic, political) depends on the hacker'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

Attackers took control of the website of a regional public transport company and replaced its ticketing and scheduling information with a large quantity of pornographic material.

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 marketplace. But, in truth, this TrustedBank would be a completely fraudulent entity.

Sometimes hackers deface the content of websites for purposes of disinformation (Figure 8.12). The hacker's motivation might be, for example, to influence events, to manipulate the stock exchange, to spread uncertainty or fear, or to manipulate public opinion.

These are called *semantic attacks*. They subvert the meaning of the information content, and fall into the category of *infowar*.

These kinds of attacks are perpetrated by exploiting flaws in computer software. They exploit implementation errors in information systems. This can threaten overall security by compromising the confidentiality, integrity, and availability of personal data.

These days, the Web is often used as an application platform. Organizations adapt existing applications and reimplement them using a browser as the user interface. These web-based applications, such as fora or e-commerce applications, will have security vulnerabilities. Hence, web-based applications are becoming new targets for attackers via malicious codes that exploit known vulnerabilities.

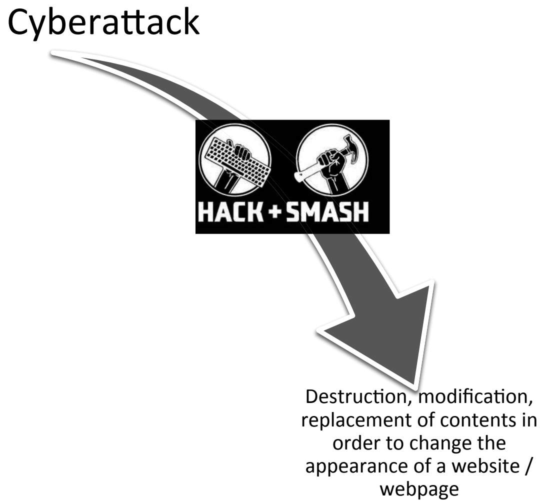

Cyberattack
HACK + SMASH
Destruction, modification, replacement of contents in order to change the appearance of a website / webpage

Figure 8.12 A defacement attack.

If they are not well protected, web-based applications are vulnerable and can expose the whole information system of an organization to cyberattacks. Common security measures, such as firewalls, however, generally allow web traffic by default. An attacker can gain access to a server – indeed, to the whole private network – by exploiting vulnerabilities in the application. After gaining access to a web server, an attacker can perpetrate a defacement attack.

Some examples of the misuse of communications protocols

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 (Figure 8.13). 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, of course, is blocked, but it is simple enough for the hacker to send a message saying that the requested system is inactive. This kind of attack is well known under the generic name of "Man-in-the-middle attack." It could apply during any protocol establishment connection's phase (TCP, SSL/TLS, HTTP, etc.).

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

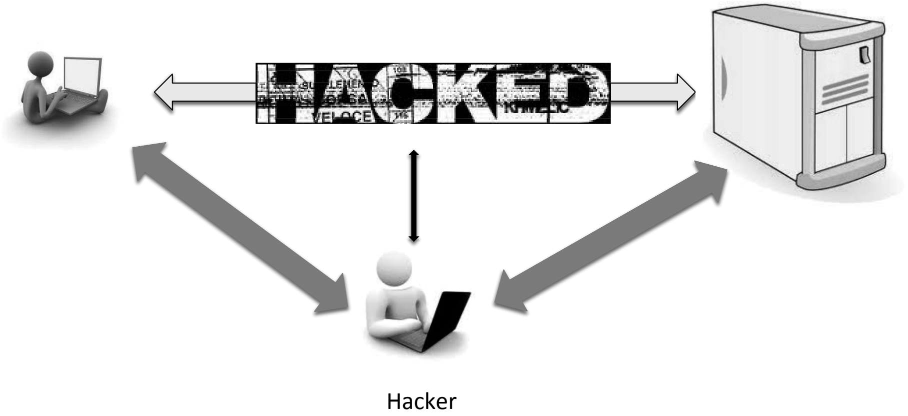


Figure 8.13 A man in the middle attack.

The User Datagram Protocol (UDP) is a transport level connectionless 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 control, or error control. 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 to confuse systems, thereby modifying packet routing and delivery by usurping IP addresses (IP spoofing), or to manipulate systems and take control of them.

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 rout-*

ing. 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, 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 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.

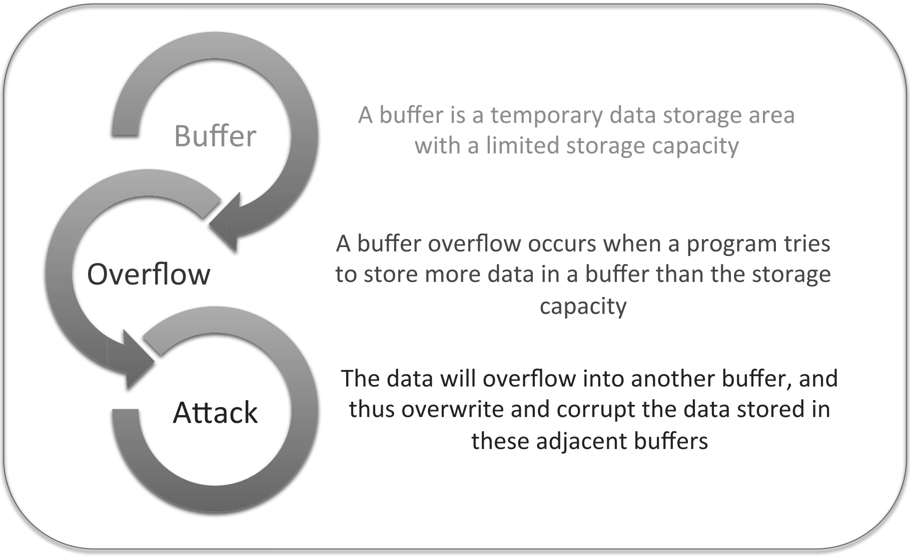
Once a hacker knows the operating mode of this public protocol, it is easy to perpetrate an ICMP attack by generating false ICMP messages. A massive number of such messages can overload the network. Flooding the network with false ICMP messages can render it unusable. Consequently, there is a need for security relating to the availability of the network and to 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).

There are few possible responses to this kind of attack apart from configuring routers 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, but this is a detective measure rather than a preventive one; that is, it will inform system managers of a problem, but cannot prevent that problem from arising.

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 (Figure 8.14). 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 load that overwhelms certain buffer zones. 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) use secure operating systems; (ii) use non-permissive configuration; and (iii) have an effective management plan.



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

Figure 8.14 A buffer overflow attack.

8.6 The black market of cybercriminality

From self-service to private underground sites

Professional cybercriminals are organised according to the specific roles they play and the input they can have within their different methods of going about their business.

Figure 8.15 sets out how the different players are linked and how the lifecycle of cybercriminal activities is structured. In this we can distinguish, in broad terms, between the processes, the tools, the skill-sets, and the different players involved in each of the phases of preparation, performance, and commercialisation of cyberattacks.

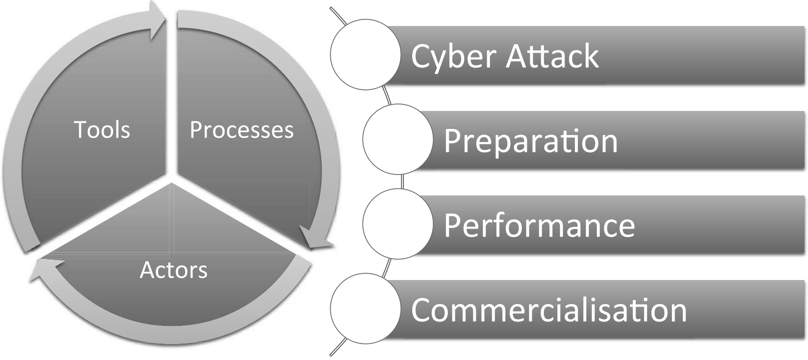


Figure 8.15 The chain of players involved in cybercriminal activities.

As we saw in Chapter 7, the population of cybercriminals is considerably heterogeneous. Exactly as in traditional criminality, there are beginners, small-time crooks, part-timers, and professional, experienced criminals. They do have one thing in common: the possibility of accessing the wide range of tools available on the Net for launching cyberattacks. These tools can be more or less conspicuous and easy to acquire; some are free, others require payment. Thus there is a genuine black market for cybercriminality on the Internet in which different types of services and tools can be obtained.

Figure 8.16 points out the different phases and links between vulnerabilities discovery and obsolescence, the creation and distribution of malware, and the correlation between the factors time and value.

Based on the type of the offer, the quality of the tools provided, and the specific nature of the target market (ranging from the seriously professional to the amateur via the young apprentice), these black market sites can be easy

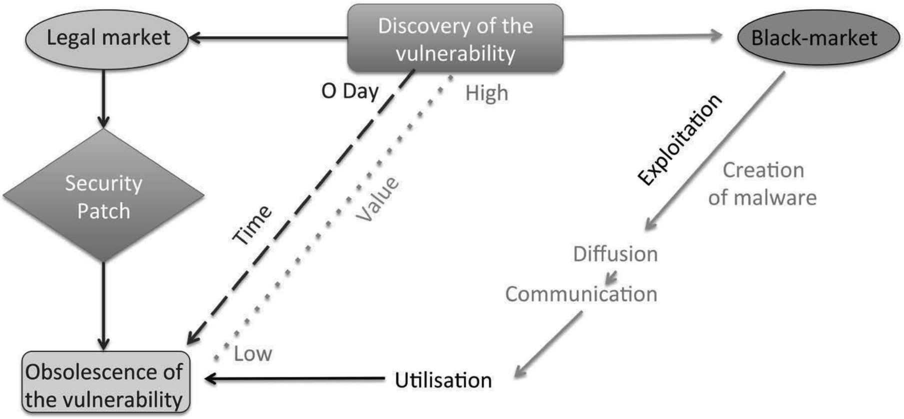


Figure 8.16 Vulnerability and malware lifecycle.

or tricky to locate. Some are freely accessible, while others, often those particularly prized for the quality of the tools and information available, operate under restricted access, reserved for regular customers or clients who have been recommended or introduced, in the same way as contacts are made in mafia circles. These sites generally require subscription, with access being managed and user activities scrutinised. These sites thus form a source of income and profit for the criminals who run them: tools and knowledge in the domain of cybercriminality fall squarely into the framework of traditional criminality and the aim for maximum profits. At the same time, as examples of illegal activities, these sites are by necessity closely monitored by their owners in order to avoid infiltration by the police and other elements of the justice system. For the majority of these sites, to which access is granted by introduction, new joiners are expected to provide evidence of their cybercriminal skills and benefit from several introductions from members of the fraternity who could vouch for them.

Overall, though, a large rage of tools is available to every Internet user, allowing novices to take their first steps in the domain by giving them the necessary means. For some, this makes the step from theory to practice very straightforward.

Different types of sites linked to the cybercriminality black market

The cybercriminality black market is based around forums and commercial sites.

Discussion forums, sometimes multilingual but most frequently in English or in national languages (Russian, German, French), are places where cybercriminals can meet and exchange information. (Figure 8.17).

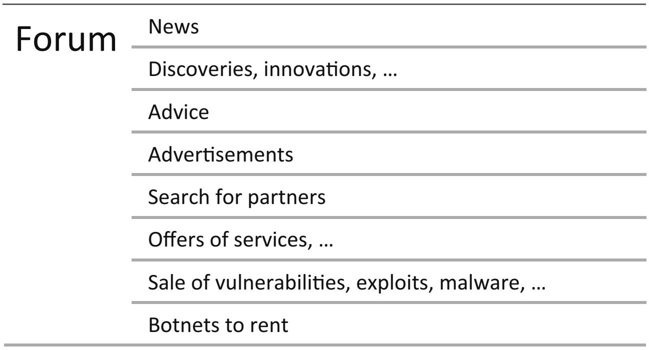


Figure 8.17 The types of services offered on, and users of, forums for cybercriminals.

Very often these forums are structured around different sub-forums, such as:

- latest news and recent exploits;
- discoveries and innovation;
- advice;
- advertisements;
- the search for partners and accomplices;
- offers of services, frauds and opportunities to collaborate;
- the sale of exploits, malware and crimeware;
- the availability and renting of botnets;
- offers to host illegal contents and launch spam.

Depending on their roles and on how important they are to the forum, users may have differing access rights linked to their status as sellers, frequent users or guests. In the same way as for classical forums, there are also administrators and moderators and means of evaluating the quality of participants. The forums provide a platform for organising and planning cybercrimes, finding the necessary skills and accomplices for a project – in the same way that legitimate businesses operate. It is often through forums that contact is made between the worlds of traditional criminality, terrorism, and cybercriminality. Conversations can be public or private and generally rely on instant messaging facilities.

Example

ShadowCrew was a cybercrime message board (forum) that operated under the domain name ShadowCrew.com between August 2002 - October 2004. […] The ShadowCrew website also contained a number of sub-forums where the latest information about hacking tricks, social engineering, credit card fraud, virus development, scams, and phishing.[10]

Commercial sites are not significantly different from legitimate e-commerce sites, and some of these demonstrate a real flair for marketing. Buyers go there, open a secured account, have access to a shopping basket, and manage their purchases.

Among the products available for purchase are:

- stolen credit card data, such as names, addresses, card numbers, expiry dates, and security codes;
- email addresses and turnkey spam services[11];
- login details, including account numbers, for online banking and for online gaming (often acquired through phishing);
- scans of genuine identity papers, of falsified identity papers (sent by actual couriers if purchased), and of fake diplomas;
- various pieces of malware that are immediately usable, giving rise to the concept of CaaS – Crimeware as a Service); this software can include phishing kits, Trojan horses, ransomware, viruses, spyware, etc.;
- hosting services for illegal content, command & control servers for botnets, and access to bulletproof servers[12];
- courses on becoming cybercrimnials or in improving skills, such as in creating better frauds or creating botnets.

Example

Welcome to DarkMarket – global one-stop shop for cybercrime and banking fraud – Personal data and tutorials in hacking offered online […] *DarkMarket price list* – Trusted vendors on DarkMarket offered a smorgasbord of personal data, viruses, and card-cloning kits at knockdown prices. Going rates were:

[10] http://en.wikipedia.org/wiki/ShadowCrew

[11] Certain spam services allow the users to sidestep measures such as Captchas (Completely Automated Public Turing test to tell Computers and Humans Apart). These are interactive mechanisms based around a challenge and a response between an information system and a human to ensure that the end-user of the service is a human being and not a piece of software.

[12] Servers located in countries where there are no legal or police measures that allow the server owners to be convicted, the servers shut down, and their users prosecuted. No legal recourse is possible, and the renting of server space and the hosting of data and programmes (spam, phishing, etc.) is provided without any concern as to their contents and purpose.

Dumps Data from magnetic stripes on batches of 10 cards. Standard cards: $50. Gold/platinum: $80. Corporate: $180.
Card verification values Information needed for online transactions. $3-$10 depending on quality.
Full information/change of billing Information needed for opening or taking over account details. $150 for account with $10,000 balance. $300 for one with $20,000 balance.
Skimmer Device to read card data. Up to $7,000.
Bank logins 2% of available balance.
Hire of botnet Software robots used in spam attacks. $50 a day.
Credit card images Both sides of card. $30 each.
Embossed card blanks $50 each.
Holograms $5 per 100.[13]

Exactly as in traditional areas of commerce, there are sites that sell to consumers and sites that sell in bulk to providers (that is to other cybercriminals), taking a margin for doing so.

The prices can vary from one site to another depending on the reseller, on the nature of the data in question (for a bank card, for example, it will hinge on the country of issue; and for account numbers it will depend on the amounts available in the account), and on the quantity purchased. Of course, some offers can very well themselves be scams set up specifically to profit from the greed of other crooks, for example by selling fictitious or faulty goods or services. Some cybercriminals can be doubly dishonest. They make use of weaknesses in electronic commerce, such as the absence of physical contact in transactions, in order to steal from the thieves. This is one of the reasons why the idea of introductions and vouching for others is so important in the cybercriminal underground; it helps to create a certain level of trust between criminals, to identify members liable to cause problems for the community, and avoid police intervention.

Sometimes commercial sites complement their offerings with the additional service of verifying the quality of the information they are selling – the idea of *checkers*. These can take the form of pieces of software or links to specialised sites that allow the validation of bank card numbers, for example, so that the potential user can be sure that the numbers are genuine and also know whether the card is subject to the Visa Verified or Mastercard Secure Code schemes.

[13] http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley; 14 January 2010

Example

Carderplanet was a criminal organization that operated and maintained the website www.carderplanet.com for its criminal activities and was founded in May 2001. By August 2004, the site had attracted more than 7,000 members. The site provided its members with a marketplace for millions of stolen credit card accounts. Although most of the postings on the forum were in Russian, and most of Carderplanet members were from Eastern Europe and Russia, the forum had a significant English-speaking component.

The Carderplanet criminal organization was organized similar to the mafia with the highest-ranking members, or "the family," having titles such as the Godfather and "capo di capi" (or boss of all bosses). Senior members of the organization shut the website down in the summer of 2004 following some arrests of high-ranking members and law enforcement scrutiny.[14]

The rubrics for "job offers and opportunities" on such sites give a good idea of the specialisation of participants in cybercriminality and of the skills required and in demand.

In principle cybercriminals are specialised, and it is not uncommon to find on their forums advertisements looking for partners or accomplices for specific activities that require multiple technical skills and experience. This splitting of skills and responsibilities (creating malware, accessing systems, hosting contents, usurping identity, money laundering) means that the gangs can reduce the time taken to carry out an operation and thereby diminish the risks of being discovered, and also reduce the likely penalties if caught and convicted.

The forums make easy the creation and maintenance of contacts at an international level, meaning that gangs can consist of people from different countries who might not even know each other offline but who can act together at a global scale.

Example – A real case

A man who created a website trading in stolen financial information linked to tens of millions of pounds in losses has been jailed for nearly five years. Renukanth Subramaniam, 33, founded Darkmarket, a "Facebook for fraudsters" where criminals could buy and sell credit card details and bank log-ins. The site was shut down in 2008 after an FBI agent infiltrated it, leading to more than 60 arrests worldwide. Subramaniam admitted conspiracy to defraud at Blackfriars Crown Court. He also

[14] http://itlaw.wikia.com/wiki/Carderplanet

pleaded guilty to mortgage fraud. ‘One-stop-shop’ Judge John Hillen said: “Criminals should learn from this case that, even in cyberspace, there is no hiding place.” Prosecutor Sandip Patel said the case was “extraordinary” because it was founded and promoted over the Internet. “They were able to utilise modern technology in a way which gave them the capability to commit theft on an unprecedented scale… with no more than a dishonest will, a laptop, a mouse and Internet access,” he said. “In short, it was a Facebook for fraudsters. John McHugh created fake credit cards that were sold through the site. Suspects linked to the website were arrested in the UK, US, Canada, Germany, France, Turkey and Russia. It even operated a secure payment system, allowing users to “review” the criminal services on offer – creating a “one-stop-shop for criminals the world over.” Subramaniam, originally from Sri Lanka, was given British citizenship in 2002 and ran Darkmarket from an Internet cafe with the username “Jilsi.” He owned three houses but lived nomadically – staying with friends mainly in Wembley, north London and Ilford in Essex. He was sentenced to 46 months for conspiracy to defraud and 10 months for five counts of mortgage fraud, the terms to run consecutively. Also sentenced was Darkmarket user John McHugh, 66, of Doncaster, South Yorkshire, who had the sign in “Devilman” and created fake credit cards that were sold through the site. He was jailed for two years for conspiracy to defraud. Investigations in the UK were led by the Serious Organised Crime Agency (Soca). Deputy director Sharon Lemon said: “Subramaniam went to great trouble to hide his activity. He seems to have thought that carrying data around on memory sticks and using Internet cafes would somehow protect him from scrutiny. He was wrong.”[15]

Communication and e-commerce tools for criminal activities

Instant messaging services allow rapid links and interactions between people. These technologies have been massively adopted by the criminal community, as services such as ICQ[16], for example, allow for anonymity, an issue much appreciated by those involved in illegal acts. The criminals can communicate with each other in identifying themselves not by a name or a pseudonym, but by a number. It is very hard to identify an individual on the basis of an ICQ number. This technology is also very useful in the commercial sites and the forums to talk with or enter into contact with advertisers, customers, people offering after-sales services, or potential buyers in certain circumstances, ICQ can itself be used as a commercial site.

[15] http://news.bbc.co.uk/2/hi/8539680.stm; 26 February 2010.

[16] ICQ is an instant messaging computer program, which was first developed and popularized by the Israeli company Mirabilis, then bought by America Online, and since April 2010 owned by Mail.ru Group. The name *ICQ* is a homophone for the phrase “I seek you.” This is an adaptation of the Morse code callout “CQ,” which means “calling any station.” Source: Wikipedia

In general, criminal use services or web platforms or instant messaging systems provide security, anonymisation, and the encryption of communication – services such as Jabber.[17] Among other functionalities, Jabber enables the creation a web server, communications with other Jabber servers, and connection to ICQ. Certain web platforms allow the instantaneous and, if necessary, temporary creation of web servers, based on specific needs. This dynamic aspect of the web facilitates reactivity and the rapidity of criminal activities, while at the same time limiting the extent to which their creators and users are vulnerable to legal consequences.

Most of the time the closure of a site is not a problem for the criminals. They have the resources to open others and to transfer contents from one server to another and from one country to another, all the while continuing their activities.

Virtual money

It is difficult to calculate with any accuracy the financial flows generated by cybercriminality. Either they are unknown or they are estimated after the fact when arrests are made, with all or part of the revenues remaining hidden or invisible or having already been reinjected into the legal economy.

In addition, the majority of financial transactions linked to cybercriminality are made instantaneously and anonymously using the facilities provided by virtual money, making traceability almost impossible.

It is thus that "Liberty Reserve," a company based in Costa Rica, acquires, through its virtual money and related service, a layer of protection for all of its money transfers across the Internet, including those related to criminal activities. Users are identified by account numbers. Money transfers are instantaneous and anonymous, without any information on the account holders – there is no verification of identities or of the sources of funds. Opening an account with Liberty Reserve is swift and simple, and can be done from an email account created specifically for that purpose. The processes for opening accounts, managing balances, and making transfers are completely opaque to outsiders. The company also offers security services to its clients.

[17] Jabber (http://www.jabber.org/create-an-account/) or the Russian site THESECURE.BIZ (http://www.thesecure.biz/index.php)

The Liberty Reserve virtual money system

Liberty Reserve is a private currency exchange system issued by Liberty Reserve S.A. of San José, Costa Rica. The two Liberty Reserve currencies are Liberty Reserve USD (LRUSD) and Liberty Reserve EURO (LREUR). Liberty Reserve S.A.'s terms of service reads:

1.7. Liberty Reserve (LR): means the digital currency in which the electronic transfer services are provided; *backed by United States of America Dollars and Euros*; hereinafter for all legal purposes referred to as LR.

Liberty Reserve is a digital currency used frequently for adding funds to and withdrawing funds from Bitcoin exchange markets.

Transfers charged by Liberty Reserve are a flat 1% to the recipient of the funds. The fee is rounded up to the nearest penny, so the minimum fee is $0.01. The maximum fee is $2.99 so essentially fees are only charged on the first $300 of any transfer.

If you are transferring LR from your account with a merchant, that merchant may charge a fee for that withdrawal, however that fee is withdrawn before the merchant sends the funds to your Liberty Reserve account.

In some circumstances, if you will be transferring LR funds from one merchant to another, you might be able to skip treating your LR as a hub and just transfer funds directly from one merchant to the other. This will save on the fee that would have been charged on the second transaction.[18]

An example of services offered by Liberty Reserve

Quick payments – An easy access to your funds to make payments quickly. This feature allows you to make quick payments without accessing your main Liberty Reserve account. Just set daily, weekly or monthly limit of funds you wish to use for handy Quick Payments and do transfers to your partners quickly and safely. *Private payment option* – Unique to Liberty Reserve, truly private payments.

You now have the option of making your payment to any other account without revealing your account number – recipient will not see the account number you have sent funds from. *Free private messaging* – Your Liberty Reserve account is not just for sending or receiving payments. Create an account and use the built-in messaging system to privately send and receive messages from your friends and business associates. This is much more private and secure than email or instant messenger services. […].[19]

[18] https://en.bitcoin.it/wiki/Liberty_Reserve. This page was last modified on January 24, 2012

[19] Liberty Reserve, S.A. (Headquarter San José, Costa Rica); http://www.libertyreserve.com/

Other systems of virtual money do exist or have existed. A good example is *E-gold*, which offered virtual money and related services that were heavily used by cybercriminals, particularly from 1996 to 2007. The company was found guilty of money laundering, as the IDG article below explains. The cybercriminals who used its services then headed towards other service providers, such as Liberty Reserve and WebMoney. WebMoney, which was originally set up in 1998 to serve Russian clients, went on to attract an international clientele of online gamblers.

The E-Gold affair

> *Internet currency firm pleads guilty to money laundering*
> E-Gold, an Internet-based payment service, and three owners have pleaded guilty to criminal charges related to money laundering, the U.S. Department of Justice. […] E-Gold, based in Nevis, West Indies, and corporate affiliate Gold & Silver Reserve each pleaded guilty in U.S. District Court for the District of Columbia to conspiracy to engage in money laundering and conspiracy to operate an unlicensed money-transmitting business. […] The resulting lack of oversight and required procedures created an atmosphere where criminals could use "e-gold," or digital currency, essentially anonymously to further their illegal activities, the Department of Justice said. […] E-Gold provided digital currency services at E-gold.com and Omnipay.com. Users did not have to provide their identities, and E-Gold continued to allow accounts to be opened without verification of user identity, despite knowing that "e-gold" was being used for criminal activity, including child exploitation, investment scams, credit card fraud and identity theft, the Department of Justice said. E-Gold assigned employees with no prior experience to monitor hundreds of thousands of accounts for criminal activity, the agency said […].[20]

About WebMoney

> Welcome to WebMoney Transfer – the global settlement system and environment for online business activities, established in 1998.
>
> WebMoney Transfer Technology is based on providing all its users with unique interfaces that allow to operate and control individual property rights for valuables (assets), stored at the specialized entities – the Guarantors.
> All Guarantors – participants of the System are located in various jurisdictions and store valuables of various legal nature. Specific features of transactions with proprietary rights for values stored by each Guarantor, as well as their measurement units and the Guarantor's obligations to exchange those proprietary rights with the

[20] http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering; 22 July 2008.

> currency of the country of its registration, are set out in the Agreements adopted respectively by every member of the System in the course of registering a 'Purse,' which serves as the accounting attribute of the proprietary rights.
>
> All Purses in the System have a 12-digits identification number and a prefix, belonging to a corresponding Guarantor.
>
> The System supports several types of Purses, that keep record of valuables property rights of corresponding types:
>
> - R-Purse WMR – Bearer's bank cheque in Russian Rubles
> - Z-Purse WMZ – Goods certificate, in USD
> - E-Purse WME – Bearer's bank cheque in EUR
> - U-Purse WMU – Bank account claims in UAH
> - B-Purse WMB – Electronic Belorussian Roubles
> - G-Purse WMG – Warehouse receipt for stock Gold in a certified storage area
> - V-Check WMV – Prepaid transfer in Vietnamese Dongs
>
> The units of measurement of the valuables' property rights stored by the guarantor are WebMoney Title Units (WM) of the corresponding type.
>
> System Users can open as many purses from any Guarantor as needed, that is why Purses belonging to one User are combined into a single repository (Keeper) under a unique identification number – WMID. WMID operation modes description, as well as conditions of its usage, are described in the Agreement on Property Rights Transfer, which is accepted by every member who joins the system.
>
> WMID allows the System's member not only to perform operations with Purses, but also to exchange legally binding messages with other members and enter into contracts.[21]

Money exchange companies

Money exchange companies are essential intermediaries for criminals who need to hide the identity and the source of their funds. These companies are heavily solicited to maintain accounts at Liberty Reserve, for example, to withdraw money or to make anonymous purchases online, without leaving any traces and without any risk.

There are many such companies, the most widely used of which have global coverage and easily-reachable offices or access points in places such as newspaper kiosks, train stations and tobacconists. Notable among these are UKash and Western Union,[22] which are legitimate businesses used for legal activities as well as for illicit ones.

[21] Webmoney http://www.wmtransfer.com/ (Feb, 19, 2012)

[22] "The Western Union Company is a financial services and communications company based in the United States. Its North American headquarters is in Englewood, Colorado. Up until 2006, Western Union was the best-known U.S. company in the business of exchanging telegrams." http://en.wikipedia.org/wiki/Company_%28law%29

About Ukash

> Ukash is designed to enable you to use your banknotes and coins to pay or send money on the internet. You don't need a bank account or credit card to use Ukash. You simply need to have some cash! […]
> Our customers tell us that they use Ukash for many different reasons. Some don't like using their bank or credit cards online. Others may not have access to a bank account. Still more like the control that Ukash gives them, as you can only spend up to the value of your Ukash voucher. […] Whatever your reason, you can get and use your Ukash without providing us with any financial information. So you stay private when you are using your money online. Read on for more information on how it works. […] Ukash is regulated by the Financial Services Authority in the UK and operates under license in 6 continents.[23]

8.7 Summary

A number of methods exist for gaining access to systems by deception. These methods are based on the vulnerabilities of the different Internet environments and on certain characteristics of the implementation and use of the protocols, operating systems and processors, as well as on the configuration and (faulty) management of the systems connected to the Internet. Hacking is therefore often simply a question of using available information.

Carrying out attacks based on deception relies upon the usurpation of identity, of login information, and of IP addresses (IP spoofing); upon changes made to routing (re-routing data flows); upon the theft of TCP connections; or on the re-routing of application data flows. These attacks exploit the intrinsic properties of the various communications protocols used across the Internet.

At the same time, many attacks consist of the modification of the welcome page of a website (defacement attack). The pirates replace the official content of the site with, according to their motivations, different types of content, such as political or pornographic materials. The consequences of such attacks for the victims can be very significant in terms of loss of image and other indirect losses. Reputations can be permanently tarnished, especially if confidence is a fundamental element of the strategic positioning of the target (such as banks or hospitals). More lucrative variations on this kind of attack set out to redirect the user, perhaps through a phishing attack, towards a fake site that exactly resembles the original site that the user was looking for. The fake site will then

[23] http://www.ukash.com/global/en/home.aspx; 19 February 2012.

be used to obtain confidential information (passwords, credit card numbers) from the user.

It is possible to attack information sites and to modify the contents of certain pages or information flows in order to provoke panic reactions or cause a fluctuation in a company's share price, for example. These activities of disinformation fall into the category of *infowar* and allow the performance of *semantic attacks*, thus having an impact on the information and beliefs that everybody uses as a basis for judgement. The possibilities for manipulating opinions are thus infinite and can have consequences of greater or lesser importance for the individuals, organizations, and states that ultimately pay the price. Certain manipulations of information can undermine the integrity or honesty of a person.

It is always important to link any discussion of security and criminality to the context of the society in which events are taking place. In this way, the context of the economic battle in which companies and institutions are engaged, both nationally and internationally, will not be forgotten. Cybercriminality is above all an economic criminality that manifests itself within a general context of a war of, through, and for information.

DoS and DDoS attacks are intended to cripple system resources. They typically operate by overloading a server with requests for the services it is designed to provide, 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 is what makes a DoS or DDoS attack so difficult to identify and to prevent.

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. Phishing attacks have become one of the most significant online security threats. Phishers aim to steal confidential information for financial crimes or identity theft, to install malware, and extend zombie networks, causing substantial financial losses and personal damage.

An attack may include a step that involves the explicit or tacit approval of the user, particularly in relation to adware. Whatever the means used to infect a user's machine, once installed, malware is turned to illicit use. Most commonly, however, a malware attack is executed without the consent of the user. It collects and transmits data clandestinely – for example, on web-surfing 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 master these risks.

Cybercriminals know how to hide behind multiple technical, organisational, and human intermediaries. They can benefit from:

- the intangible nature of players, transactions, and services;
- the international reach of the Internet that allows them to act at a distance, far from their physical location;
- services permitting anonymisation and instant exchanges of information;
- the facilities offered by e-commerce, virtual money, and money exchange companies;
- the facilities offered for money laundering across the Internet.

8.8 Exercises

1. What are the principal types of attack that can be performed over the Internet?
2. What are the principal dangers linked to electronic mail in the context of cybercriminality?
3. What are the main success factors for carrying out an attack?
4. Why is it beneficial for a security manager to be familiar with the different phases of the performance of an attack?
5. Is it easier to detect a passive or an active attack? Why?
6. What are the advantages to spear phishing as opposed to phishing?
7. Where does usurpation of identity fit into the performance of cyberattacks? What advantages can it bring?
8. How can virtual money help cybercriminality?
9. What is a Trojan horse? How does it differ from a virus?
10. What is meant by the term "malware attack"?
11. What is a Denial of Service attack?
12. What are the key characteristics of a defacement attack?

13. Why can the misuse of Internet communications protocols present a problem?

14. What is the role of legitimate money exchange and transfer companies in cybercriminal activities?

15. Which Internet communications services are the most favoured by cybercriminals?

16. What are the roles of "mules" in cybercriminality?

17. What are the characteristics of social engineering?

18. How can cybercriminals benefit from the existence of social networks?

19. How can the cybercriminal underground exploit opportunities offered by the Internet?

20. Which tools are most frequently used in the cybercriminal black market? Describe both the roles they play and the advantages they provide.

Chapter 9

The Fight Against Cybercrime

9.1 Understanding the context

To prevent, deter, and fight cybercrime, the underlying cyberthreats and the nature of cyberattacks should be well understood. If justice wants to pursue cybercriminals, it is not sufficient merely to know the motivations and general means of operating of cybercriminals; it is also necessary to recognize and monitor illicit activities and have the means to identify and pursue criminals involved in these activities. To accomplish this, it is important to possess appropriate means in each of the organisational, legal, procedural, technical, and human domains. Key assumptions related to this are that:

- There exist channels for recognizing and reporting cybercrimes;
- This is supported by an appropriate legal framework and organizational structures;
- The structures, procedures, staff and tools employed in IT-based investigations are useable and practical;
- The cooperation and sharing between the different elements of the police services and the justice system are effective and efficient at both the national and international levels.

The majority of countries have now implemented organisational structures that allow the reporting and recording of cybercriminal activities. As an example of this, the centre for recording and analysis of information security of the

Swiss confederation in Bern, MELANI,[1] provides users with forms to report offences and regularly publishes a status report on those incidents. In addition, information and advice on protecting computers is provided, and an information letter is published to inform readers of problems and possible solutions.

Although reports on computer crimes are regularly published by diverse institutions, such as the SCOCI[2] in Switzerland, the National Fraud Authority in the UK,[3] the Internet Crime Complaint Center (IC3) in the USA,[4] and the Canadian Anti-Fraud Centre,[5] the few reliable statistics and identification of trends that emerge from them reflect only the visible part of the iceberg of cybercriminality.

Over recent years the number of security incidents reported to CERT,[6] for example, has been growing steadily. Both the increasing complexity of these incidents since the start of the current century and increased reporting has contributed to a better understanding for authorities of the scale and significance of computer crime. However, the number of infractions committed but not reported to the justice services and the police is considerable. The hidden aspect of cybercrime, which represents the number of crimes and offences unknown to the police services because no complaint has been made, demonstrates the gap between known malevolence and real malevolence. It is often impossible to estimate the size of this gap in any realistic way.

Because ICT related crimes are frequently unreported and the useful information related to cybercrime is often incomplete, it is difficult to obtain an accurate estimate of the size of this phenomenon. This forms a real obstacle to the analysis of cybercrime and contributes to the misunderstanding of both its importance and its impacts. It is also difficult, in this context, to find the financial, organizational and human means to fight it. This could lead to under- or over-estimating the scale of cybercrime, both of which would complicate the task of developing effective, efficient, and appropriate counter-security measures.

[1] Within MELANI, the Reporting and Analysis Centre for Information Assurance, partners work together who are active in the area of security of computer systems and the Internet and protection of critical national infrastructures. http://www.melani.admin.ch/index.html?lang=en

[2] Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) – http://www.cybercrime.admin.ch/kobik/fr/home.html

[3] http://www.actionfraud.org.uk/news

[4] http://www.ic3.gov/default.aspx

[5] http://www.antifraudcentre-centreantifraude.ca/english/home-eng.html

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

As a confounding factor, the research on the quantification of cybercrime emerging in particular from players in the computer security market should also be treated with caution as a consequence of the sampling techniques employed, the dynamic nature of the subject matter, and the motivations of the companies. These analyses can be seen as being a barometer of the security situation, an indicator of tendencies, but also a marketing tool to support the sale of the latest solutions. This caution is a necessary response to potentially misleading information.

Available statistics do illustrate how the security measures put in place by organizations tend to provide protection for a given environment in a particular context, but are often helpless to prevent criminal activity via the Internet. The reasons for this state of affairs are related, in particular, to the following:

- the nature of cybercrime and its trans-national dimension which requires international assistance and judiciary cooperation;
- the ease and impunity with which criminals can usurp legitimate user identities, use anonymising techniques, and employ multiple technical and geographical intermediaries, thereby thwarting the ability of the legal system to identify the authors of a criminal act;
- the need to resolve the territorial issues before conducting an investigation;
- the lack of human, procedural and technical resources within the services responsible for anti-cybercrime work and computer investigations.

For all of these reasons, cybersecurity measures often remain ineffective. The proliferation of computer-related crime is not necessarily, however, a sign that there are not enough laws. Existing laws already cover many cybercriminal activities, but it is simply very difficult to bring cybercriminals to justice.

9.2 Strengthening legislation is not enough

It is not enough simply to attempt 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 analysing evidence, and identifying and prosecuting the perpetrators of criminal acts. If cybercriminals are confident that they will escape punishment, that is a strong indication that the system is ineffective. At the same time, as shown in the following examples, there are still many cases of cybercrime being solved by police forces all around the world.

From Interpol

Hackers reportedly linked to 'Anonymous' group targeted in global operation supported by Interpol

LYON, France – An international operation supported by INTERPOL against suspected hackers believed to be linked to the so-called 'Anonymous' hacking group has seen the arrest of some 25 individuals across four countries in Latin America and Europe. Operation Unmask was launched in mid-February following a series of coordinated cyber-attacks originating from Argentina, Chile, Colombia and Spain against the Colombian Ministry of Defence and presidential websites, as well as Chile's Endesa electricity company and its National Library, among others. The international operation was carried out by national law enforcement officers in Argentina, Chile, Colombia and Spain, under the aegis of INTERPOL's Latin American Working Group of Experts on Information Technology (IT) Crime, which facilitated the sharing of intelligence following operational meetings in the four participating countries. Some 250 items of IT equipment and mobile phones were also seized during searches of 40 premises across 15 cities during the operation, as well as payment cards and cash, as part of a continuing investigation into the funding of illegal activities carried out by the suspected hackers who are aged 17 to 40. "This operation shows that crime in the virtual world does have real consequences for those involved, and that the Internet cannot be seen as a safe haven for criminal activity, no matter where it originates or where it is targeted," said Bernd Rossbach, Acting INTERPOL Executive Director of Police Services.

INTERPOL working parties on IT crime were created to facilitate the development of strategies, technologies and information on the latest IT crime methods. There are regional working parties for Africa, the Americas, Asia and the South Pacific, Europe, and the Middle East and North Africa. The main activities of the working parties rest on three pillars: facilitating operations against IT crime among INTERPOL's 190 member countries, capacity building and addressing emerging threats.[7]

Large-scale police operations carried out in several countries have shown that the authorities are indeed reacting and adapting to the new criminal context. The arrest and conviction of several virus authors, spammers, and data thieves, can testify to the determination to deal with these new types of nuisances. However, the number of convictions remains very low, given the sheer volume of spam and viruses circulating on a daily basis.

[7] http://www.interpol.int/News-and-media/News-media-releases/2012/PR014; February 28, 2012.

Examples

Spammer Sentenced to Nine Years in Jail
A brother and sister were convicted this week of three felony charges of sending thousands of junk e-mails through servers located in Virginia.[8]
A man who claims to be the "*Godfather of Spam*" has been sentenced to 51 months in prison by a federal judge in Detroit for his lead role in an e-mail stock scam scheme, according to court documents [...][9]

Spam king rules prison cell for 11 years
[...] According to court documents, T.M. and A.V. had devised a way to defeat AOL's filtering system. During one week in August 2005, the two of them managed to target over 1.27 million AOL e-mail addresses with spam. The indictment accuses of them of violating a section of the CAN-SPAM Act that says that "the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period." The charges appear to be limited solely to the activities involving the government informant, despite the pair's long track record with spam. [...] T. M. was caught bragging to the informant about the money he was making: as much as $40,000 per week. Pump-and-dump stock e-mails were the most lucrative [...]. With the potential profits so great and hordes of botnets available to do much of the dirty work, it's no wonder that spammers have been largely undeterred by legislation such as the CAN – Spam Act (USA – *C*ontrolling the *A*ssault of *N*on-*S*olicited *P*ornography *A*nd *M*arketing – 2003).[10]

Computer virus author jailed
A man who admitted infecting thousands of computers across the world with fast-spreading viruses has been jailed for two years. S.V., 22, created the viruses at his home in Llandudno, North Wales, and released them on to the internet. The "mass-mailer" viruses were sent as e-mails that would corrupt data on the computer's hard-drive when they were opened. In addition, the viruses were automatically sent to everyone on the computer's address book [...] S.V. made the e-mails tempting to computer users by using subject lines such as: "You have a secret admirer." Another message alluded to Vallor's interest in a British pagan religion, which read: "Bide ye the Wiccan laws ye must, in perfect love and perfect trust."[11]

[8] http://www.pcworld.com/article/118493/spammer_sentenced_to_nine_years_in_jail.html; November 5, 2004

[9] http://money.cnn.com/2009/11/24/technology/King_of_spam_lawsuit_fraud_Ralsky/ November 30, 2009

[10] http://arstechnica.com/tech-policy/news/2007/06/spam-king-may-rule-prison-cell-for-11-years-after-feds-nail-him.ars

[11] http://news.bbc.co.uk/2/hi/uk_news/wales/2678773.stm; January 21, 2003

Melissa virus author jailed for 20 months
The author of the infamous Melissa virus was sentenced today to 20 months in Federal prison for causing millions of dollars of damage through its release into the wild in March 1999. […] D.L.S., 33, pleaded guilty to creating the virus in December 1999 – the delay in his sentencing has created consternation in the security community. […] Both sides in the case agreed that damage from Melissa, one of the first email borne viruses that exploited flaws in Microsoft's Outlook client exceeded $80 million, largely by jamming up corporate email systems […][12]

Heavy sentence given to creator of 'ika-tako' virus
The Tokyo District Court on Wednesday sentenced a 28-year-old man to two years and six months in prison without suspension on charges of property destruction for creating a computer virus, spreading it on the Internet, and damaging data in infected computers. This is the first time that property destruction charges have been applied to a computer virus creator.[13]

Sasser virus author arrested
In what the company called a «coordinated multinational law enforcement effort,» information provided to Microsoft by informants led local authorities to arrest the 18-year-old unnamed resident of Rotenburg, Germany, only a week after the original Sasser virus had been released. […] Microsoft's $5 million fund for rewarding informants for leads on virus attacks has snagged its first success with the arrest of a man in Germany who has confessed to the release of the Sasser worm, the software giant said Saturday. […] The arrest is the first success for Microsoft's Antivirus Award Program, a $5 million fund to reward people for coming forward with information about those who release major worms and viruses. While Microsoft has offered three rewards for $250,000 each for those who were responsible for the havoc caused by the MSBlast worm, the Sobig virus and the MyDoom virus, no arrests in those cases have yet been made. The arrest of the author of a minor variant of the MSBlast worm predated the award program.[14]

Operation Ghost Click – International Cyber Ring That Infected Millions of Computers Dismantled
Six Estonian nationals have been arrested and charged with running a sophisticated Internet fraud ring that infected millions of computers worldwide with a virus and enabled the thieves to manipulate the multi-billion-dollar Internet advertising industry. Users of infected machines were unaware that their computers had been compromised – or that the malicious software rendered their machines vulnerable to a host of other viruses. […] Beginning in 2007, the cyber ring used a class of malware called DNSChanger to infect approximately 4 million computers in more than 100 countries. There were about 500,000 infections in the U.S., including

[12] http://www.theregister.co.uk/2002/05/01/melissa_virus_author_jailed/; May 1, 2002
[13] http://www.yomiuri.co.jp/dy/national/T110720005908.htm; July 21, 2011
[14] http://www.internet-security.ca/internet-security-news-005/sasser-virus-author-arrested.html May 10, 2004

> computers belonging to individuals, businesses, and government agencies such as NASA. The thieves were able to manipulate Internet advertising to generate at least $14 million in illicit fees. In some cases, the malware had the additional effect of preventing users' anti-virus software and operating systems from updating, thereby exposing infected machines to even more malicious software[…][15]

Few statistics are available on cybercrime, and most incidents are not reported to the police. Also, since criminal legislation tends to be national, and infractions are taking place across borders, it is difficult to compile statistics on crimes that might be defined differently from one country to another. For example, in 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 either as computer-related crime or as financial crime.

The rate of unreported cybercrime is difficult to estimate. It is possible that the legal authorities, the police, and the general public are aware, of no more than a small pourentage – maybe between 10% and 20% of cybercrimes. It is difficult to obtain a realistic inventory of computer-related crime, and this is a serious obstacle to analysing the phenomenon and determining its magnitude.

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

- wish to avoid publicity about attacks. They do not want to reveal that they have been victims of cybercriminal acts, as this could reveal their technological vulnerabilities or security weaknesses and could lead to negative publicity that would benefit competitors. It is not always easy for a victim to report a crime, sometimes for fear of appearing ridiculous, sometimes for not wanting to damage a brand (a person, an enterprise), sometimes because of a feeling that doing so is useless, or sometimes because the process seems too complex;
- may be unaware that they have been the victims of cybercrime, particularly in the case of passive attacks (transparent hijacking of data, traffic, passive listening, undetected intrusion, etc.); they may also not learn of the attack until much later, when there is no point in reacting. Awareness of having been attacked can require sophisticated monitoring processes: it is rapidly obvious when systems are taken offline or data are destroyed; less obvious when data are modified, depending on the extent; but not necessarily obvious at all when data are neither modified nor destroyed. How will a company be aware that a system has

[15] http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911; November 9, 2011

been used as a temporary intermediary to perform a money laundering action over the Internet, if the tracks have subsequently been removed?

- do not know how to deal with a crisis situation or to report a cybercrime;
- do not have any obligation to complain (to report the incident);
- lack the necessary confidence in the legal authorities and police and in their ability to deal with this type of problem, even if it is seen as significant enough to investigate;
- prefer to handle such matters themselves, perhaps even in the sense of meting out their own justice, illegally, by attacking the systems and resources that attacked them.

Hackers' interpersonal skills, the sophistication and potency of attacks, and the quality and availability of attack toolkits are improving all the time; in addition, the actual quantity of attacks continues to grow. The ever-increasing complexity resulting from this dynamic trend is difficult for law enforcement to handle. Without a strong political will and a sense of responsibility among all participants at the international level, as well as an effective partnership between the private and public sectors, any security measures, whether of a technical or legislative nature, will not constitute any more than an inadequate and piecemeal approach to security, and thus will remain ineffective in tackling computer-related crime.

9.3 An integrative approach and a global strategy

In a global strategy, fighting cybercrime essentially involves:

- increasing the level of effort the criminal must exert to commit a crime;
- increasing the level of perceived risks;
- decreasing expected profits.

In order to reach these generic goals, cybersecurity measures have to be put in place (Figure 9.1). For example, with regard to the level of effort needed to carry out an attack, potential targeted resources can be less vulnerable if there are access control, integrity control, authentication control, or monitoring mechanisms.

In a complementary approach, legislative and regulatory measures contributing to law enforcement can help to raise the level of risk perceived by a criminal. These could contribute to restricting cybercriminal activities to some kind of manageable level.

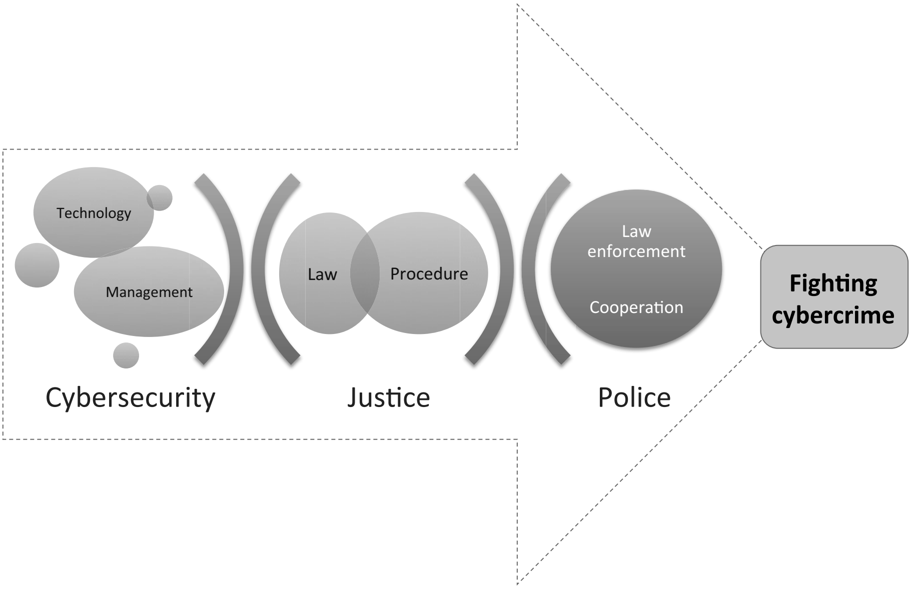


Figure 9.1 A complementary and integrative approach.

A relevant international reference on cybercrime legal issues could be found in the Convention on Cybercrime of the Council of Europe. The convention identifies cybercrimes that should be prosecuted and gives direction on investigating such crimes. The problem of international cooperation is also addressed.

The Council of Europe Convention on cybercrime

On November 8, 2001, the Council of Europe adopted the Convention on Cybercrime (ETS n°185)[16] and its Explanatory Report;[17] these were proposed for signature on November 21 in Budapest on the occasion of the International Conference on Cybercrime. Ten years on, this convention constitutes a reference document that contributes to fostering and providing guidance on developing national legal frameworks and supporting international cooperation in the fight against cybercrime.

The regional initiative of the Council of Europe Convention on Cybercrime is an example of legal measures. For countries that have not ratified it

[16] www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[17] www.conventions.coe.int/Treaty/en/Reports/Html/185.htm

yet, it could be seen as a guideline and a set of principles that can be a source of inspiration when they do develop their internal legislation.

The following section presents a brief summary of the Convention. It is not intended to provide an exhaustive commentary on each of the aritcles, nor any kind of legal analysis. Readers interested in the detail should refer to the text of the Convention itself.

After a brief definition of terms in the Convention on Cybercrime Chapter I, Chapter II defines measures to be taken at the national level and deals with substantive criminal law (Section 1), procedural law (Section 2) and jurisdiction (Section 3).

Several types of offences are presented and classified under four titles in Section 1, namely:

- 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).

Section 1 defines various computer or computer-related crimes that should be punishable under criminal laws.

The convention specifies offences against the confidentiality, integrity and availability of computer data and systems (Section 1, Title 1) related to:

- illegal access (Art. 2);
- illegal interception (Art. 3);
- data interference (Art. 4);
- system interference (Art. 5);
- misuse of devices (Art. 6).

Title 2 concerns computer-related offences and makes the distinction between:

- computer-related forgery (Art. 7);
- computer-related fraud (Art.8).

Content-related offences are treated in Title 3 and concern offences related to child pornography (Art. 9).

The criminalization of xenophobic acts committed through computer systems is treated by the additional protocol to the Convention on Cybercrime (EST 189). "*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."[18]

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.

Offences related to infringements of copyright and related rights are described in Title 4 – Article 10.

Additional offences related to attempting to commit or aiding and abetting offences, as defined in the Convention, are also punishable, and the question of indirect liability is raised. Attempts to commit and aiding or abetting (Art. 11) as corporate liability (liability of a legal person) (Art. 12) are integrated in Title 5 – Ancillary liability and sanctions. Sanctions and measures (Art. 13), which end the first section, are related to consequences flowing from the serious nature of these offences by providing for criminal sanctions that are effective, appropriate, and dissuasive. Quoting directly from the Convention:

> 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.

The explanatory report on Convention on Cybercrime[19] introduces 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.

[18] EST 189.Definition – page 3.

[19] www.conventions.coe.int/Treaty/en/Reports/Html/185.htm

Section 2 begins with two general provisions that apply to all the articles relating to procedural laws (Title 1 – Common provisions Articles 14. 15), while Title 2 concerns "expedited preservation of stored computer data." A distinction is made between computer and traffic data as reflected in Articles 16 and 17:

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

Article 18 (title 3) deals with the notion of production order. A "production order" provides a flexible measure which 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.[20]

Article 19 – "Search and seizure of stored computer data" (Title 4) aims at modernising and harmonising 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.[21].

Article 20, "Real-time collection of traffic data," and Article 21, "Interception of content data," make up Title 5, "Real-time collection of computer data," and address the problem of the real-time collection of traffic data and of the interception of content data by competent authorities, as well as their collection or interception by service providers. Obligations of confidentiality are also addressed. The section on "jurisdiction" mentions that each party is required to punish the commission of crimes, established in the convention, that are committed in its territory.

Principles related to international cooperation, extradition and mutual assistance are given in Chapter III. Procedures pertaining to mutual assistance requests in the absence of applicable international agreements are also defined.

[20] www.conventions.coe.int/Treaty/en/Reports/Html/185.htm (p.27).

[21] www.conventions.coe.int/Treaty/en/Reports/Html/185.htm (p.30).

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

Regarding substantive criminal law, the convention covers:

- offences against the confidentiality, integrity, and availability of computer data and systems;
- computer-related offences;
- offences related to infringements of copyright and related rights.

In regard to procedural law, the convention covers:

- expedited preservation of computer and traffic data, and rapid disclosure of the latter to the competent authorities;
- preservation and maintenance of the integrity of computer data for a period of time, as long as is necessary to enable the competent authorities to seek its disclosure;
- production order;
- search and seizure of stored computer data;
- real-time collection of computer data;
- the adequate protection of human rights and liberties.

Each state has to adopt the necessary legislative and other measures to establish jurisdiction over the following offences, without prejudice to its domestic law:

- when committed intentionally, the access to the whole or any part of a computer system without right;
- when committed intentionally, the interception without right of non-public transmissions of data to, from or within a computer system;
- when committed intentionally, the damaging, deletion, deterioration, alteration, or suppression of computer data without right;
- when committed intentionally, the serious hindering without right of the functioning of a system;
- the production, sale, procurement for use, import, distribution, or otherwise making available of a device designed or adapted for the purpose of committing any of those offences;
- when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic;
- when committed intentionally and without right, the causing of a loss of property to another person by any input, alteration, deletion or

suppression of computer data, or any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person;
- establish as criminal offences the aiding or abetting of any of those offences, and any attempt to commit any of those offences.

Each of the signatories has to establish jurisdiction over any offence committed:

- in its territory;
- on board a ship flying the flag of that country;
- by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any state.

Rules on international cooperation relate to:

- extradition;
- mutual assistance for purposes of investigation;
- procedures for criminal acts related to computer systems and data;
- collection of electronic evidence of a criminal act.

A mutual assistance network is to created:

- that is available on a 24/7 basis;
- with a national point of contact; and
- with immediate assistance with offences.

The European Convention on cybercriminality obliges the countries that have ratified it to establish a national point of contact, available 24/7 (Article 35), a central authority responsible for sending and receiving extradition requests (Article 24), and support for legal cooperation (Article 27).

Whatever the national legal system and related practices in each country, criminal laws should punish, for example, illegal access to or interception of data, interference with systems or data, misuse of devices, computer related forgery and fraud, offences related to child pornography, phishing, botnets, spam, and identity theft.

In order to criminalize cybercrime, some countries will have to adapt (or have already adapted) the scope of their legislation. Below is presented a non-exhaustive list of applicable legal domains:[22]

[22] The list of proposed law domains cannot be exhaustive because: (a) each country has its own law structure and names; (b) differences in the interpretation of cybercrime may exist between countries; and (c) laws must be adapted to the dynamic nature of the evolution of technology.

- penal;
- civil;
- commercial;
- telecommunication;
- privacy and data protection;
- copyright;
- unfair competition;
- banking and professional secrecy;
- right of disclosure/access;
- statuary obligations for storage/disclosure;
- accounting;

From the Chairman of High Level Expert group of ITU GCA

> Moreover, countries should establish the procedural tools necessary to investigate and prosecute cybercrime, as described in the Convention on Cybercrime Articles 14-23. International coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments.[23]

The need for efficient approaches to policing and applying justice

Fighting against cybercrime means that secure technical barriers must be effective to increase the level of difficulty of attacking a system. Performing a malevolent act becomes more complex, and the chances of carrying it out successfully are reduced. However, this is not enough if the criminal still feels that he or she can act with impunity. If the objective is truly to increase the level of risk taken by the criminal, the criminal must absolutely understand that he is carrying out a malicious and illegal act. Laws must exist, therefore, to criminalize illicit behaviour, and members of the justice system and police forces should have the means to identify criminals and bring them to justice with an appropriate sentence.

[23] Judge Stein Schjolberg – Perspectives on cybercrime laws based on ITU – GCA – HLEG recommendations – p.19. EWI Cybercrime Legal Group, 2011.

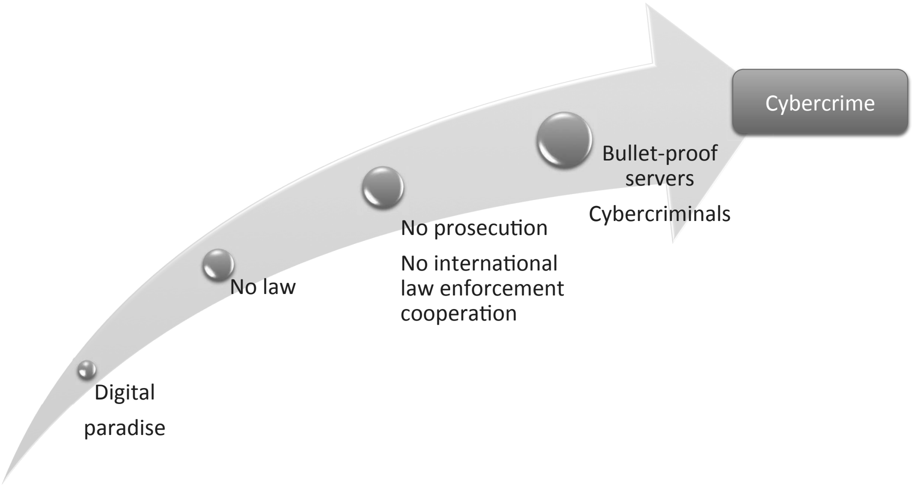


Figure 9.2 – Digital paradise.

A nation's ability to deter, detect, investigate and prosecute cybercriminal activities is one of the most important components in providing secure information infrastructures and stability. Because of the international nature of the Internet, vulnerabilities and weaknesses could compromise the security of others all around the globe. The absence of applicable and enforceable laws in a country leads to the creation of *digital paradises* used to develop harmful activities (Figure 9.2).

The consequences of a digital paradise are prejudicial for all concerned. Each country should address cybersecurity and cybercrime issues and not become the weakest link in the chain of global security. Each country has to apply appropriate technical measures and adopt an enforceable legal framework. That means that specific criminal laws must exist, and police forces must have the capacity to investigate and pursue computer-related crime. The justice system and the police should be able to rely upon an adequate organizational structure and upon trained personnel with specific technical competencies and sufficient means, even if individual cybercrimes might have a relatively weak impact on each individual victim.

In most developed countries these last points are not always particularly well addressed, due to the lack of financial resources allocated to fighting cybercrime, the lack of technical capacities, of competencies and organizational structure of the police forces, an absence of interest in cybercrimes – most of which are not viewed as being very serious (lacking physical violence), and also because cybercrimes can be very difficult to resolve.

As stated at the beginning of this chapter, to prevent, deter, and fight cybercrime, cyberthreats and cyberattacks should be well understood. To pursue cybercriminals, it is not sufficient to recognise cybercriminals' motivations and their modus operandi if society as a whole is unable to supervise and recognize illicit activities and discover criminals. To achieve that, trained specialists, tools and procedures for cybercrime pattern recognition, for taking charge of digital evidence and performing computer investigations, should be operational and effective.

Understanding a cybercriminal's motivation and level of technical skills can help to assess how serious an attack is, and assist in devising a counterstrategy. It could also be useful when trying to identify him during a police investigation (Figure 9.3).

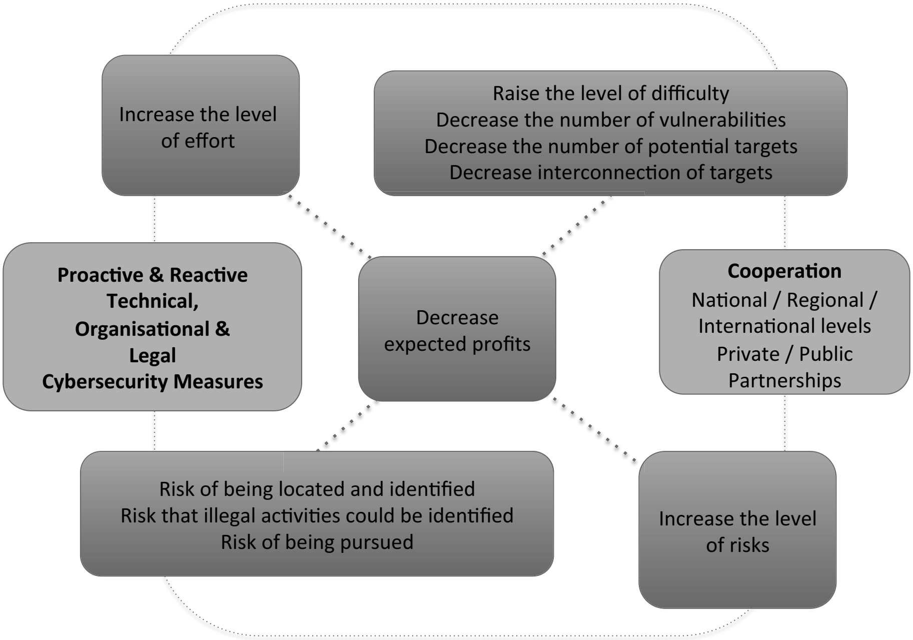

Increase the level of effort
Raise the level of difficulty
Decrease the number of vulnerabilities
Decrease the number of potential targets
Decrease interconnection of targets
Proactive & Reactive Technical, Organisational & Legal Cybersecurity Measures
Decrease expected profits
Cooperation
National / Regional / International levels
Private / Public Partnerships
Risk of being located and identified
Risk that illegal activities could be identified
Risk of being pursued
Increase the level of risks

Figure 9.3 The main aspects of an integrated global approach.

In terms of international cooperation, certain countries can establish bilateral or multilateral conventions for legal matters, as well as agreements on judicial cooperation and extradition.

At the same time it will be necessary to clearly define the rules relating to national jurisdiction to enable cooperation to go ahead rapidly and efficiently, both at national and international level.

Unmasking cybercriminals

Understanding cybercriminal profiles and motivations can be a great help in protecting information technologies and pursuing cybercriminals.

At the present time, as we have seen in Chapter 7, there are two main groups of cybercriminals: the professionals who make money from their work, and the amateurs, who tend to be persons with a pronounced need for recognition.

Computer-related crime is sophisticated, and is very often committed across national borders. The traces it leaves in computers are intangible and difficult to gather, collect, securely save, or understand. They take the form of digital information stored on all sorts of media, sometimes all around the world. The problem lies in how to identify, locate, and collect digital evidence when carrying out cybercrime investigations.

The following questions illustrate the extent to which the concept of digital evidence remains elusive:

- How to identify the relevant data?
- How to trace them?
- How to store them?
- What are the judicial rules of evidence?
- How to recover files that have been deleted?
- How to prove, without ambiguity, the origin of a message?
- How to establish the identity of a person on the basis of only a digital trace, in view of the difficulties of reliably linking digital information with its physical author (virtualization) and the proliferation of identity theft?
- How to establish the conclusiveness of digital evidence in establishing the truth before a court (concept of digital evidence), knowing that the storage media from which the evidence has been recovered are not infallible (date-time information being treated differently from one computer system to another, and subject to tampering)?

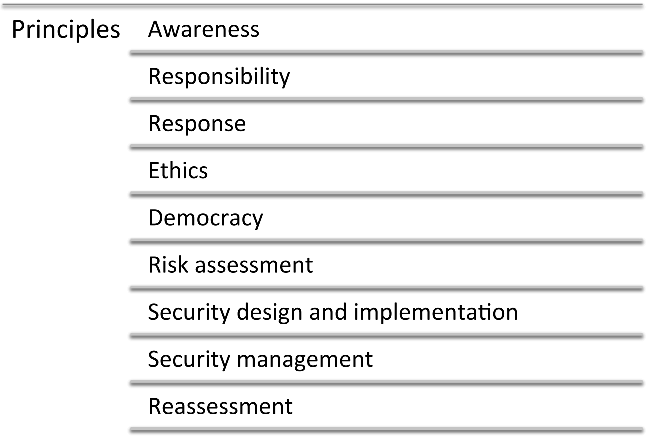
Digital evidence is even more difficult to obtain when it is scattered across systems located in different countries. In such cases, success depends entirely on the effectiveness of international cooperation between legal authorities and the speed with which action is taken. Effective use of such evidence to identify individuals depends on the speed with which requests are treated: if treatment is slow, identification is next to impossible.

In most countries there is a significant mismatch between the skills of the criminals who commit high-technology crimes and the resources available to the law enforcement and justice authorities to prosecute them. The use of computer technologies by those authorities, whether at the national or international level, remains weak and varies greatly from one country to another.

In most cases, the police and judicial authorities rely on the conventional investigation methods used for ordinary crime to identify cybercriminals and build up cases against them.

Strengthening international cooperation and law enforcement

In order to be effective, the fight against cybercrime should rely upon a strong political will at both the national and international levels. The problem is not always linked to the absence of laws or guidelines, as this absence can be addressed with reference to materials 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" (Figure 9.4). Rather, difficulties arise from the difficulty and complexity of the task, and the resources necessary to effectively combat not only cybercrime but also organized crime and institutional corruption.



Principles	Awareness
	Responsibility
	Response
	Ethics
	Democracy
	Risk assessment
	Security design and implementation
	Security management
	Reassessment

Figure 9.4 OECD principles for information security (July 2002).

New technologies are not the remote and secretive domain of a group of scientific visionaries whose sole objective is mankind's improvement. Delinquents adapt to any new environment and take advantage of it to carry out and improve their traditional activities. There is legitimate cause for alarm that these individuals and organizations can be so perversely creative when it comes to inventing insidious new uses for these technologies. For example, criminal organizations did not wait until Europe and the US agreed on the future standards for mobile telephony to adopt the mobile phone.

It would be dangerous for police forces to postpone developing competencies and assigning resources to investigate computer crime. This would carry 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 the whole range of possible destabilizing effects that would accompany these.

However, a colossal increase in police or military presence on the network is not necessarily the best solution. It is essential to preserve the bedrock of fundamental democratic principles throughout cyberspace.

As is the case for all security activities, the struggle against cybercriminality is based on political willingness and needs to follow a global approach that corresponds to a shared vision of public security, so as to provide efficient and effective protection for citizens, countries, and the fundamental values of democratic societies. The protection of fundamental rights includes, specifically, the protection of personal data and the protection of individuals in respect to the automated processing of personal data. It will be necessary, then, to acquire the means to implement a genuine security response, rather than to create a pseudo-security framework based on excessive social control that increasingly relies upon sophisticated and virtually invisible electronic surveillance – methods that reduce individual freedoms in the name of a relative collective security.

One of the major matters at stake in the fight against cybercriminality is the development of a genuine information culture that is not simply focused on security and based on fear. With cybersecurity it is not sufficient to make the population aware of the dangers of the Internet and the elementary precautions to be taken. Essentially all the players, i.e. all the service and technology providers, will need to accept responsibility for their role in the global and collective struggle.

Mounting an effective response to cybercriminality is based upon developing a preventive approach that will make cyberspace a less attractive environment for committing crimes and also reduce the number of opportunities for criminal activities. To achieve this, it will be necessary to increase the level of difficulty of carrying out cyberattacks and increase the risks taken by criminals in going about their business (dissuasive measures), while all the time decreasing the expected profits. This kind of approach will require both reducing technical, organisational, and human vulnerabilities in order to increase the level of effort, difficulty, and investment required by the criminals, and possessing and knowing how to use the tools, procedures, and measures necessary to increase the risk for the criminals that they will be identified, localised, and pursued.

Therefore, it will be necessary to reinforce the robustness and the resilience of IT and telecommunications infrastructures by reducing their vulnerabilities, protecting them through coherent technical, procedural and managerial security measures, and having recourse to an effective justice and police system. Thus the whole process requires the combination of political will, legal, organisational, procedural, technical and human means, the establishment of partnerships between the public and private sectors, and good international cooperation.

9.4 The principal challenges in combating cybercrime at the international level

Capacity building

Effectively combating cybercrime requires a legal framework that has been harmonized at the international level and that can be applied effectively and equally. It also requires true international cooperation at the level of the police and justice authorities.

National governments are responsibe for ensuring the stability of cybersecurity and cyberspace. This is particularly true not only in defining a suitable legal framework, that is, one that is enforceable at a national level and compatible at the international level, but also in relation to the promotion of a security culture.

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 and the protection of fundamental human rights. As shown in Figure 9.5, the main actors involved in the fight against cybercrime can be classified as:

- the protector (private and/or public institutions);
- those to be protected (the individual citizen, the organisation, and the State);
- the criminal (professional or not).

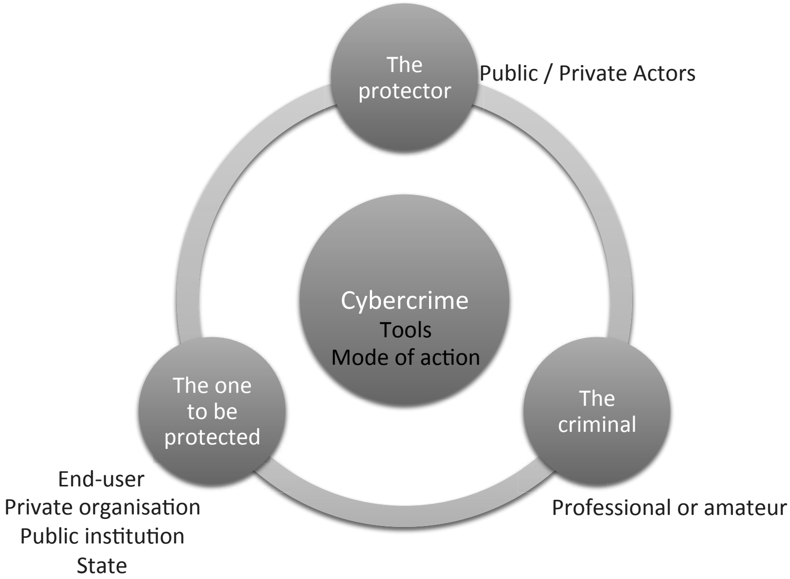


Figure 9.5 Interrelation between the different kinds of actors involved in the fight against cybercrime.

However, security is not just a cultural problem that has a technological dimension. It is also a regulatory issue. A cyberspace regulatory framework could help to transform the Internet into a safer place to conduct activities. A legal framework that is applicable to the digital world must be operational at the national and international level. Security solutions can protect a given environment in a particular context, but cannot prevent criminal behaviour altogether. Legal institutions and the law itself exist to counter both of these aspects to dissuade criminal behaviour and to bring individuals who carry out illegal acts to justice.

Officers of justice and police authorities who are skilled in new technologies and cybercrime need to enforce the legal aspects of ICTs and cooperate with their partners at the international level.

States need to develop within their societies a confidence in ICTs that can be comparable to its confidence in air transportation. This is only possible:

- through implementing tight and rigorous control processes;
- by ensuring that security measures are implemented with total transparency.

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

- understands cybercrime from a global perspective;
- develops public awareness of cybercrime and cybersecurity challenges, including economic and management issues, political issues, social issues, technical issues, legal and law enforcement issues;
- promotes a cybersecurity culture by providing information on stakes and risks, and publishing simple recommendations, such as the use of secure systems and the reduction of vulnerability by avoiding dangerous situations or behaviours;
- trains and informs citizens and organizations on ICTs, security issues, and relevant legal provisions;
- develops cybersecurity education;
- proposes a unified and harmonized e-security framework, that includes the human, regulatory, organizational, economic, technical, and operational dimensions of cybersecurity;
- creates effective cybercrime laws that are enforceable at the national and international levels; this means developing a global and harmonized legal framework that takes into account the right to privacy (protection of public safety with protection of privacy and civil liberties);
- creates regional centres for the provision of technical information and assistance regarding security risks and cybercrime;
- manages jurisdictional issues;
- fights cybercrime through a whole range of measures and practices, including the following: deterrence, detection, investigation, prosecution, crime reporting, crime analysis, search and seizure of digital evidence, information sharing, and promotion of effective public and private sector cooperation;
- redefines law enforcement and legal frameworks to more effectively bring cybercrime perpetrators to justice;
- develops acceptable practices for IT protection and reaction;
- promotes and establishes effective cooperation and coordination among all relevant actors;
- sets higher standards for ICT and content providers regarding the security of their products and services; providers must integrate simple and flexible security measures and mechanisms into their products or services; products should be well-documented and comprehensible;

> security mechanisms should be readily understood and easily configured by untrained users; security must be integrated at the beginning of ICTs' infrastructure development life cycles.

The justice and police authorities need to be able to rely upon competent staff. This emphasises the increasing need to be able to provide specialised training, often of an interdisciplinary nature, for judges, magistrates, lawyers, and police officers.

Cybersecurity constitutes a driving force for the economic development of regions and must be implemented simultaneously with ICT infrastructure. Security needs should be answered at the same time as other ICT development activities.

An inclusive society would be able to avoid the pitfalls of creating digital paradises or allowing a situation of exclusion from digital security. The digital divide should not be aggravated by a security divide (Figure 9.6).

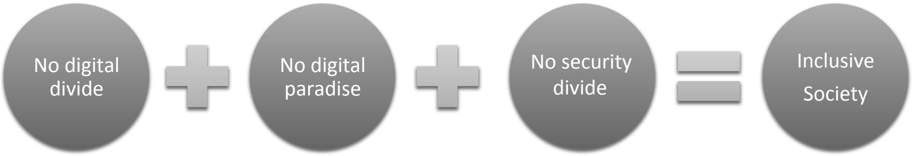


Figure 9.6 An inclusive society: all united against cybercrime.

When a country becomes a digital paradise or the "weakest link" in the international security chain, that affects the overall, global level of cybersecurity.

Individuals should be at the heart of the ICT security question to help create an inclusive information society. It is illusory to think that technological or legal solutions would be able to compensate for design or management errors whether they occur at a strategic, tactical, or operational level. The legal and technological world must be in harmony. Technology is not neutral, nor is the law.

It is essential that the development of the legal and technological worlds follows economic development, and that these factors become a driving force for the economy. Building humain capacity is a tool among others to contribute to build an inclusive information society.

A question of means, willingness and organizational structures

Much as with the struggle against global warming, the fight against cybercriminality is the subject of summit meetings and political debates. The World Summit on the Information Society (WSIS),[24] among other initiatives, contributed to identifying the need for Internet governance at a United Nations level and the requirements for securing an Internet that would be more reliable and more accessible to the whole population, including developing nations. International resolutions have been adopted to develop cybersecurity and fight against cybercriminality. In the same light, the International Telecommunications Union, through its "*Global Cybersecurity Agenda*,"[25] a programme launched in 2007 that tackles in a global manner the problems of cybersecurity, published a strategic report as a reference document and contributed to the creation in Malaysia in 2009 of the IMPACT (International Multilateral Partnership Against Cyber Threats) centre, dedicated to countering cyberthreats.[26] Elsewhere, in 2008 NATO (the North Atlantic Treaty Organisation) decided to create in Estonia a training centre for protection against electronic attacks over the Internet. Although it would be impossible to list here all the institutions concerned by the management of information security and the struggle against cybercriminality, we should mention in this context ENISA (the European Network and Information Security Agency) and the OECD (Organisation for Cooperation and Economic Development)[27] that offer activities, events, publications and directives in these fields.

Fundamentally, however, these recommendations and structures cannot replace a real political desire or the genuine mobilisation of all the players, public and private. It is the essential role of these players to get organised and work together in order to implement means of protection and reactions that are consistent, coherent, and complementary.

The scope of unblocking funds to implement a well-defined strategy, one that is based on feasible security policies, is not restricted to financing security technologies, such as access control methods. As discussed above, in order to be able to report and investigate crimes and identify and pursue their perpetrators, there is a need for an efficient organisation encompassing all the necessary elements (justice services, police, other law enforcement bodies,

[24] The WSIS took place in two phases, the first in Geneva in December 2003, and the second in Tunis in November 2005; http://www.itu.int/wsis/index.html

[25] http://www.itu.int/osg/csd/cybersecurity/gca/

[26] http://www.impact-alliance.org/

[27] http://www.enisa.europa.eu/ and http://www.oecd.org/

intelligence, civil defence), to specify the appropriate procedures, and handle questions of territorial responsibility and liability.

For example, regarding the French institutions involved in the fight against cybercriminality, one notes the *Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication* (O.C.L.C.T.I.C.), which is part of the *Direction Centrale de la Police Judiciaire*. This office works closely with, among others, the *Direction Centrale du Renseignement Intérieur*, the *Direction Générale de la Sécurité Extérieure*, the *Direction de la Protection et de la Sécurité de la Défense*, Interpol and Europol, and is at the same time the national point of contact for countries that have ratified the Convention on Cybercriminality. In addition, in the context of certain investigations various other police units, the *Gendarmerie Nationale* or the Customs may be invited or required to work alongside these other bodies. This is also the case regarding investigations requiring specific technological competences, tools for collecting and analysing digital traces, or for recovering data from damaged or blocked sources, such as hard disks or data cards.

The entities that are dedicated to the identification and pursuit of criminals intervene after the event, in response to the reporting of a crime. Crime prevention depends on structures for monitoring and informing, such as CERT/CC[28] (Computer Emergency Response Team/Coordination Center) and CSIRT (Computer Security and Incident Response Team[29]). These are organisational structures that play a key role in anticipating crime by detecting faint signals that are the precursors of large-scale attacks. These bodies are also active in the field of publicising the discovery of new weaknesses, security solutions, practical recommendations, and knowledge about the management of risks of crises.

As a general rule, most countries do possess national structures along the lines of CERT and/or CSIRT, bodies that may or may not be members of the FIRST forum (Forum of Incident Response and Security Teams).[30] There are also regional CERTs, such as, for example:

[28] http://www.cert.org/

[29] "CSIRT provides 24x7 Computer Security Incident Response Services to any user, company, government agency or organization. CSIRT provides a reliable and trusted single point of contact for reporting computer security incidents worldwide. CSIRT provides the means for reporting incidents and for disseminating important incident-related information." (http://csirt.org/)

[30] FIRST "brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large". http://www.first.org

- APCERT – Asia Pacific Computer Emergency Response Team;[31]
- EGC – European Government CERTs Group.[32]

These structures can also be supported, in certain countries, by monitoring and alert-giving networks, often collectively known as Watch and Warning Networks (WWN). These are often partnerships between the public and private sectors and can operate at a national or international level.

International cooperation regarding cybercriminality relies upon organisational structures that allow direct contact, twenty-four hours a day and seven days a week, between the different specialised police units. Among the major players at an international and European level in the struggle against cybercriminality are:

- Interpol;
- Europol (European Police Office);
- Eurojust (European Union Judicial Cooperation Unit).

About Interpol

> INTERPOL is the world's largest international police organization, with 190 member countries – Our role is to enable police around the world to work together to make the world a safer place. Our high-tech infrastructure of technical and operational support helps meet the growing challenges of fighting crime in the 21st century […] At INTERPOL, we aim to facilitate international police cooperation even where diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of

[31] APCERT – http://www.apcert.org/ "APCERT cooperates with CERTs and CSIRTs to ensure Internet security in the Asia Pacific region, based around genuine information sharing, trust and cooperation".

[32] EGC – http://www.egc-group.org/ "The EGC group forms an informal association of governmental CERTs in Europe. Its members effectively co-operate on matters of incident response by building upon a fundament of mutual trust and understanding due to similarities in constituencies and problem sets.
To achieve this goal, the EGC members

- jointly develop measures to deal with large-scale or regional network security incidents;
- facilitate information sharing and technology exchange relating to IT security incidents and malicious; code threats and vulnerabilities;
- identify areas of specialist knowledge and expertise that could be shared within the group;
- identify areas of collaborative research and development on subjects of mutual interest;
- communicate common views with other initiatives and organizations.

EGC is an operational group with a technical focus. It does not determine policy, which is the responsibility of other agencies within the members' national domain. EGC members generally speak for themselves and on their own behalf."

> the Universal Declaration of Human Rights. Our Constitution prohibits "any intervention or activities of a political, military, religious or racial character."
> *The vision* – what INTERPOL aspires to achieve "Connecting police for a safer world." Our Vision is that of a world where each and every law enforcement professional will be able through INTERPOL to securely communicate, share and access vital police information whenever and wherever needed, ensuring the safety of the world's citizens. We constantly provide and promote innovative and cutting-edge solutions to global challenges in policing and security. *The mission* – what INTERPOL does to achieve its vision "Preventing and fighting crime through enhanced international police cooperation." We facilitate the widest possible mutual assistance between all criminal law enforcement authorities. We ensure that police services can communicate securely with each other around the world. We enable global access to police data and information. We provide operational support on specific priority crime areas. We foster continuous improvement in the capacity of police to prevent and fight crime and the development of knowledge and skills necessary for effective international policing.[33]

The new Interpol global complex for innovation (2014) integrates the Interpol Digital Crime Centre, which is focussed on:

- boosting cybersecurity and countering cybercrime;
- managing a forensic laboratory to support digital crime investigations;
- research to test protocols, tools and services and to analyse trends of cyber-attacks;
- development of practical solutions in collaboration with police, research laboratories, academia and the public and private sectors;
- addressing issues such as Internet security governance.[34]

About Europol

> Europol is the European law enforcement agency. Our job is to make Europe safer by assisting the Member States of the European Union in their fight against serious international crime and terrorism. Large–scale criminal and terrorist networks pose a significant threat to the internal security of the EU and to the safety and livelihood of its people. The biggest security threats come from terrorism, international drug trafficking and money laundering, organised fraud, counterfeiting of the euro currency, and people smuggling. But new dangers are also accumulating, in the form of cyber crime, trafficking in human beings, and other modern-day threats.

[33] http://www.interpol.int/About-INTERPOL/Overview

[34] http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation Starting in 2014 it will be operational in Singapore.

> This is a multi–billion euro business, quick to adapt to new opportunities and resilient in the face of traditional law enforcement measures.[35]

The European Cybercrime Centre (EC3) of Europol has been operational since January 2013. It is the focal point in the EU's fight against cybercrime, contributing to its faster reaction to incidents and the identification of trends.[36]

About Eurojust

> Eurojust's core business is to assist the competent authorities of EU Member States, when they deal with serious cross-border and organised crime, such as terrorism, trafficking in human beings, drugs and arms, the sexual exploitation of women and children, cybercrime, various kinds of fraud and money laundering. Eurojust can assist in such cases where a Member State and a non-Member State are involved. It can also help a Member State and the Commission when offences affect the European Union's financial interests. […] Because crimes threatening European citizens are often global in nature, Eurojust has worked with various partners to help meet this threat. It has negotiated cooperation agreements for the exchange of judicial information and personal data outside the EU. […] Eurojust stimulates and improves the coordination of investigations and prosecutions between the competent authorities in the Member States and improves the cooperation between the competent authorities of the Member States, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests. Eurojust supports in any way possible the competent authorities of the Member States to render their investigations and prosecutions more effective when dealing with cross-border crime.
>
> At the request of a Member State, Eurojust may assist investigations and prosecutions concerning that particular Member State and a non-Member State, if a cooperation agreement has been concluded or if there is an essential interest in providing such assistance.
>
> Eurojust's competence covers the same types of crime and offences for which Europol has competence, such as terrorism, drug trafficking, trafficking in human beings, counterfeiting, money laundering, computer crime, crime against property or public goods including fraud and corruption, criminal offences affecting the European Community's financial interests, environmental crime and participation in criminal organisations. For other types of offences, Eurojust may assist in investigations and prosecutions at the request of a Member State.[37]

[35] https://www.europol.europa.eu/content/page/about-europol-17

[36] www.europol.europa.eu/ec3

[37] http://eurojust.europa.eu/Pages/home.aspx

Elsewhere at an international level, various organisations are active in the field of combatting cybercriminality are:

- General Assembly of the United Nations;[38]
- UN Offices on Drug and Crime (UNODC);[39]
- UN Interregional Crime and Justice Research Institute (UNICRI);[40]
- International Telecommunication Union;[41]
- Internet Governance Forum;[42]
- North Atlantic Treaty Organization (NATO);[43]
- Organization of American States (OAS);[44]
- Commonwealth Telecommunications Organization (CTO);[45]
- Organization for Economic Cooperation and Development (OECD);[46]
- Group of Eight (G8) Industrialized Nations;
- Shanghai Cooperation Organization (SCO);[47]
- Collective Security Treaty Organization (CSTO);[48]
- International Multilateral Partnership Against cyber Threats (IMPACT)[49].

About IMPACT

As the world's first not-for-profit comprehensive global public-private partnership against cyber threats, the International Multilateral Partnership Against Cyber Threats (IMPACT) is the cybersecurity executing arm of the United Nations' specialised agency – the International Telecommunication Union (ITU). As the world's first comprehensive alliance against cyber threats, IMPACT brings together governments, academia and industry experts to enhance the global community's capabilities in dealing with cyber threats.[50]

[38] http://www.un.org/en/ga/
[39] http://www.unodc.org/
[40] http://www.unicri.it/
[41] http://www.itu.int
[42] http://www.intgovforum.org/cms/
[43] http://www.nato.int/cps/en/natolive/index.htm
[44] http://www.oas.org/en/default.asp
[45] http://www.cto.int/
[46] www.oecd.org
[47] http://www.sectsco.org/EN/
[48] http://www.odkb.gov.ru/start/index_aengl.htm
[49] http://www.impact-alliance.org/home/index.html
[50] http://www.impact-alliance.org/aboutus/mission-&-vision.html

9.5 Some privacy related considerations

Because privacy is a real concern for end-users of the information society, and because cybercrime can have a significant impact on digital privacy, the following section will discuss the most relevant stakes, challenges, threats, and privacy issues.

Privacy definition and global approach

According to the *Oxford English Dictionary*, 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), technologies do not maintain by default the privacy of users. To mention only one example, every Internet Service Provider has the opportunity to access user contents. This affects everyone's privacy over the Internet, and can endanger e-business activities.

Copying, logging, and eavesdropping are easy to perform. Network analysis traffic, active auditing, intrusion detection systems, and firewalls, for example, can contribute to optimizing network performance and security, but, at the same time, they can harm users' privacy. The importance of Internet privacy is made increasingly clear given the wider availability of management tools, such as protocol analyzers, linked to the exponential use of e-services, and the continually growing number of Internet users. Eavesdropping, leading to the theft of personal or strategic information, such as commercial propositions, could give unfair advantage to conomic competitors.

Effective privacy and security solutions will contribute to obtaining confidence in information and communication technologies. The needs for privacy and security are not yet well-identified or satisfied for individuals and enterprises. In fact, the majority of users seem to consider that information security is restricted to the use of anti-spam and antivirus software or to the use of encryption mechanisms that guarantee the authenticity, confidentiality, and integrity of data. Frequently, privacy measures are neglected or ignored by ordinary Internet users.

The main issues in privacy

Digital traces are generated by all e-activities. These traces can be stored and handled, both on a legal and an illegal basis. Judicial and police investigations, computer forensics for commercial and marketing purposes, or state and governmental policies could all take advantage of personal data linked to digital traces to achieve specific objectives. Furthermore, illegal monitoring, illegal data acquisition, and identity theft are a common computer related crimes. Technologies such as the Internet, sensors, global positioning systems (GPS), biometrics, smart dust, cameras, and microphones are all around us. Pervasive computing is a reality. As information technology resources continue to propagate and to be interconnected, it will become possible to gather information about virtually everything and everyone, anywhere and at any time. Consequently, privacy issues are becoming an increasingly major concern for citizens and organizations within the information society.

Various sensors and daily use devices and services are increasingly capturing personal geo-data. This can be performed either with the explicit consent of the users (GPS, smartphones, social networks, web applications, etc.) or not. Various applications that make use of geo-data already exist, covering a range of military, police, marketing, and personal uses, such as retrieving a stolen smartphone, locating an elderly person or a hiker lost in the mountains, monitoring a convicted person, sending ad hoc information to fighting troops, helping people meet each other, providing city-guide information or personalized marketing, or automating supply chain management, to mention a small sample.

All these applications contribute to watching over, monitoring, and profiling people everywhere; however, at any instant, these data can also be used by anyone else who acquires them for any goal. It is easy to transform a smartphone into a "spy-phone" (environmental spying) that allows listening to all communications, reading text messages and emails, reading and deleting the data contained in the smartphone, and other invasions of privacy.

It is time to balance the added value of geotagging services to society and the risks to privacy that arise from the possible abuses and misuses of these services.

Personal geo-data and their exploitation that can be done by licit or illicit entities raises some additional challenges to data protection and privacy and also introduces geostrategic challenges in managing and controlling the movement of people and objects.

In fact, without any effective legal constraints, collecting and taking advantage of geo-data can be misused to perform real time monitoring of people and activities and to carry out privacy breaches and offences. All of these problems are going to increase because everyone is increasingly using “intelligent” tools and increasingly efficient sensors of various kinds, and also because numerous efficient systems for managing and analyzing these huge amounts of geo-data are being developed.

The concept of privacy in cyberspace now 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 creating something in another person’s name. Therefore in the Internet it is difficult, or even impossible in some cases, to prove that a person is telling the truth about his identity or claims. In addition, everyone who has access to a computer can examine the data stored on it. The digital coding of information, the dematerialization of actors, and the ubiquity of remote accesses favour the illegal access to, and copying of, data. The majority of data on computers are essentially unprotected, unless the owner takes special precautions.

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. Consideration of the nature of the personal information that is in transit (for example, medical and tax records) will inevitably lead to the universal conclusion that everybody wants, needs, and should expect privacy.

Currently, data confidentiality and privacy protection, where they exist, are provided with an absolute lack of transparency for the end-user. Security is done by obscurity. Moreover, when a website requires personal information from an Internet user, it is not evident what will happen to that information. What the websites will do with that information is not obvious. Will they share it with other entities? And, how long will they keep it? Users cannot easily see or understand the role of web cookies[51] and the information gathered by them. Very often cookies affect user privacy in one way or another. Users need to understand what cookies are used for and what that means for their personal information.

To satisfy users’ concerns, some websites have tried to make their practices more transparent. But many privacy policies are models of legalistic complexity, while others contain so little information as to be almost useless. Consequently, website privacy policies do not serve their goal of letting Internet users be informed about how their personal information is used.

[51] Web/Internet cookies are short programs used by web servers that contributes to identify and to personalize services to end-users.

Cybercrime and privacy related problems

These days cybercriminals, hackers, or crackers – whatever we wish to call them, represent a real threat to society, causing malicious harm to ICT resources, individuals, organizations, and states.

Through their ability to intercept data and to gain entry into systems and access data, cybercriminals reduce users' privacy. The deployment of phishing attacks,[52] as well as social engineering[53] techniques, contributes to end-users losing personal information (addresses, financial information, account information, passwords, etc.). This kind of information is a precious target for cybercriminals who then exploit it to perform illegal actions. The number of identity thefts is always increasing, allowing more and more frauds to be committed and impacting a growing number of users and organisations.

Since 1999, instances of digital identity theft have increased in an exponential manner. This phenomenon cannot be ignored, and in the absence of actions to protect and to dissuade, it will continue to explode. One of the most utilized methods to carry out such robberies is malevolent software (*malware*), such as viruses or Trojans. Trojans are a kind of virus that can be hidden inside data files (such as mp3 tracks, free games, pictures, movies…). Once the file holding the virus is accessed, the Trojan could provide information to the cybercriminal in a manner that is invisible to the user. Very often the Internet users have no idea that their private information has been stolen. This information could be used to perpetrate criminal actions and thus a user whose identity has been stolen could find himself responsible for malicious activities that he did not perform and of which he was not aware. In this context, he has to prove his innocence, which is difficult, or, without any help, even impossible.

The fact that security solutions cannot guarantee privacy protection leads to critical consequences, not only for the end-users but also for organizations and society as a whole.[54]

As described previously, computer related crimes are becoming significant within society. Old crimes are being committed with new technologies, and

[52] Phishing attacks aim to gather confidential information by luring the user with a message that 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.

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

[54] Chapter 12 presents the fundamentals in technical security measures.

these technologies can, in turn, lead to new crimes. Individual criminals and organized crime are taking advantage of the facilities offered by the Internet. Police investigations in information and communication environments are increasingly necessary and frequent. These rely upon computer forensic and digital trace analyses that constitute an emerging scientific police specialization. This involves both information gathering and flow and data monitoring. These processes must be well understood and managed in accordance with the fundamental principles of democracy; they raise privacy issues and need to be integrated in an appropriate legal framework enforceable at both national and international levels.

Society has to deal with a major contradiction that exists between the needs of justice and police investigation and the rights to the protection of privacy and freedom for individuals, corporations, government, and countries.

Privacy stakes and challenges

Many stakes and challenges are related to privacy protection over 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 technology resources in order to provide the minimum level of confidence mandatory for an effective digital economy. Efficient e-business and e-government activities must integrate information security and privacy solutions.

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

Privacy issues cannot be dissociated from information security issues. Concrete, simple, efficient, flexible, and comprehensible measures must be developed to contribute to building confidence in information and communication technologies and services. This constitutes a major challenge for the twenty-first century, in transforming our society into a safe and secure information society.

An enforceable legal framework must account for the need to protect privacy and security. Consistent and appropriate national, European, and international laws related to the digital world must be defined and applicable.[55]

[55] S. Ghernaouti-Hélie. (February 12, 2003) “Challenges to develop and deploy a unified e-security framework”. UNECE Workshop on E-Security and Knowledge Economy, Geneva, Switzerland.

The best way to preserve one's private life is to do not leave too much personal information on commercial servers or in social networks, virtual communities, discussion forums, or chat-rooms. Internet servers never forget, and when users provide personal data to services, applications, or servers outside their control, they never know how those data will be exploited, by whom, and for what purpose.

Internet users have to keep in mind that personal data represent a valuable asset that consequently should be well protected.[56]

In the context of police investigations and legal procedures, it is useful to have a system of rules on the protection of personal data to guarantee a certain level of protection of the fundamental rights of individuals. The rules should be respected both at a national level and in the framework of international cooperation and cross-border collaboration for policing and judicial purposes. The collection and processing of personal data should be legal, moderate, and strictly relevant to the specific purpose for which the data have been collected.

9.6 Summary

The synergies and convergence of organised crime, economic crime, and cybercrime, as well as the coming together of the terrorist and criminal worlds, necessitated a full-fledged, multilateral and transnational response to address the needs of national security and of the security of organisations and individuals.

The international recognition of the problem, which has become the subject of political and legal debates and also of technological, sociological and economic studies, has shown that cybercriminality cannot be viewed in one single dimension. Only an interdisciplinary and integrated approach to the phenomenon will enable its full comprehension and allow appropriate preventive and reactive measures to be taken; the effectiveness of these measures will depend on their completeness and consistency.

This creates a challenge that needs to be taken up rapidly, developing the necessary knowledge and attitudes towards the information society that will satisfy the need for digital security while, at the same time, respecting human rights and the democratic values of our society.

Increasing awareness among all members and stakeholders of the information society is fundamental, but it is not by itself sufficient to fight cybercrime.

[56] In September 2000, Amazon.com, Inc. declared that its customers' data were intangible assets comparable to others.

Usual security policy prevention measures consist of raising the overall level of risk taken by criminals and decreasing profitable expectations. This entails having the capacity to detect criminals' activities over the Internet, and to localizing, to identifying and pursuing criminals. To achieve this, complementary legal, organizational, and technical measures and resources should both exist and be efficient at local and international levels.

As criminals exploit Internet vulnerabilities, the existence of fewer weaknesses should decrease criminal opportunities. To realize that goal, it is necessary to improve and enforce the robustness of information technologies and the quality of the technical, procedural, and organisational measures devoted to information security. In so doing, the difficulty of carrying out an attack is increased, and the related costs in terms of efforts, means, and know-how needed to commit such an illegal act are similarly increased. All in all, a global, comprehensive, and integrative information security approach will help reduce threats and risks to the information society.

Today deficiencies still exist with respect to:

- a global and educated culture of cybersecurity for all the members of the information society;
- adequate legal, organisational, technical measures; and
- international cooperation to fight against cybercrime and enforce ICT infrastructure security.

Urgent requirements are evident at the international, regional and national levels to resolve the capacity building problem to obtain confidence and security in the use of ICTs, as identified by the World Summit on the Information Society[57] (Geneva 2003, Tunis 2005) and by the ITU Global Cybersecurity Agenda initiative, launched on World Telecommunication and Information Society Day 2007 by Dr. Hamadoun Touré, Secretary-General of the ITU.[58]

The first convention set up to address the international character of cybercrime was the Council of Europe "Convention on Cybercrime" (STCE no. 185 – Budapest 23.XI. 2001). This was adopted in Budapest on November 23, 2001, and entered into force in July 2004, following its ratification by five of the signatory countries. Three of the signatory countries were required to be from the Council of Europe.[59]

[57] http://www.itu.int/wsis/c5/index.html

[58] http://www.itu.int/osg/csd/cybersecurity/gca/docs/Brochure%20English.pdf

[59] The list of countries that have signed or ratified the CoE Convention on Cybercrime can be found at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

The countries unequipped with laws forbidding cybercriminality are *digital paradises*, where criminals can launch cyberattacks or host illegal contents with complete impunity. The differences in national legal approaches form a barrier to the fight against cybercriminality, which is, by its very nature, international. There is a need not only for a legal framework applied at a national level, but also for this framework to be compatible internationally, as has been clearly identified in the Council of Europe's Convention on Cybercriminality.

Beyond the necessary willingness to harmonise legal frameworks, individual states must also transmit their political willingness onto effective cooperation between the judicial services and the police. Thus, there is a need for organisational structures, procedures, and competent staff to make genuine international cooperation possible, as has been shown by the activities led by Interpol and Europol in the struggle against traditional criminality.

9.7 Exercises

1. What are the major difficulties and challenges of the fight against cybercriminality?
2. Which types of resources and structures are necessary to combat cybercriminality at the national and international level?
3. In what way was the European Convention on Cybercriminality novel?
4. What are the principal advantages, disadvantages, and limits of the European Convention on Cybercriminality?
5. Why has the European Convention on Cybercriminality become a global reference in the domain of the fight against cybercriminality?
6. Why should officers of the justice system be specially trained in cybercriminal matters?
7. What kinds of knowledge and technical skills related to cybercriminality should be expected of magistrates, judges and lawyers?
8. What kinds of organizational structures should exist within a country in order to combat cybercriminality?
9. What kinds of dissuasive measures should be developed in order to combat cybercriminality?

10. To combat cybercriminality what are the most important issues regarding international cooperation?

11. Why and how can a country be viewed as a digital paradise?

12. In the context of the fights against cybercriminality, what are the consequences of the existence of digital paradises?

13. Which measures could prevent the existence of digital paradises?

14. What are the principal challenges that cybercriminality and the fight against cybercriminality present to the protection of personal data?

15. In which ways can partnerships between the private and public sectors contribute to the fight against cybercriminality?

Chapter 10

The Global Cybercrime Ecosystem and Cybercriminal Investigation

10.1 Understanding the context

The challenge of estimating the size of the cybercriminal ecosystem

The process of actually implementing effective measures in the fight against cybercriminality needs to be based, on one hand, on knowledge of the key players and their motivations and, on the other, on an understanding of their means of operation. This requires understanding their strategic vision, their operational methods, their organisation, their internal structure, their recruitment of agents, their processes, their business model, their profit laundering methods, and so on.

It is difficult to provide categorical responses to many of these questions because it is in the interests of the criminals to go about their business in the shadows and with complete discretion. Obscurity, like corruption, provides a layer of protective isolation to the illegal activities carried out by criminals of all kinds.

In the case of cybercriminality, the Internet contributes massively to shielding and masking criminal activities, making their perpetrators invisible. The international nature of cybercrime, the ability of the network to allow people to act at a distance while remaining hidden behind a screen, in addition to the ability to pass through multiple technical intermediaries and the telecommunications and information infrastructures of different countries, the fact of anonymisation, the possibility of using false or stolen digital identities – these factors make it very difficult to acquire a complete, global view of the realities of cybercriminality.

Many elements contribute to the difficulty of establishing a definitive picture of those involved in cybercriminality or quantifying accurately the costs of cybercriminality to society (Figure 10.1), such as the scale of cybercriminal activities, the nature of cybercriminals, who could be Mr. Ordinary or a specialist in IT or in organised crime, passing through a range of mercenaries willing to work for the highest bidder, and the global scope for committing crimes.

At the same time, the dynamic nature of this phenomenon, in which the players are constantly reorganising themselves as a result of the opportunities that arise, prevents outsiders from gaining a clear view of its size and scope. Rather than obtaining a static perspective, trends can be identified over a given period in the perception of the phenomenon, according to chosen indicators and the results of the studies or the observations.

The majority of entities involved in information security at an international level possess their own methods for measuring and analysing cybercriminality. This is true of companies such as Verizon, Kaspersky, RSA, McAfee and PwC, to name only a few. Studies are regularly published at both a national and an international level about cyber-risks in the broadest sense; these studies present a relatively macroscopic view of the phenomenon.

There are very few studies of victimology, and when these do exist, they only consider a sample of the crimes, the perpetrators, the victims, and the countries concerned. In addition, it appears that only a small percentage of

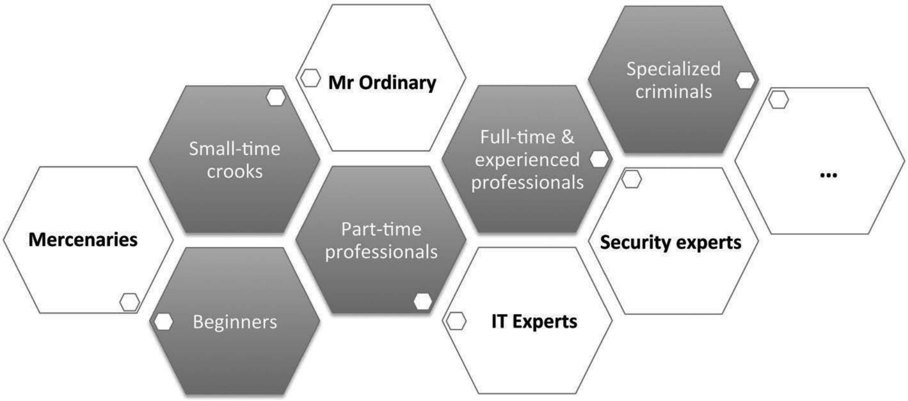


Figure 10.1 Cybercriminality: the dark side of Internet users.

cybercrimes are reported to the authorities. What's more, the theft of digital information is difficult to identify and quantify, because the data are simply copied rather than removed, as is the case in espionage, passive attacks, the abusive surveillance of activities, disinformation, and the manipulation of opinion.

The cybercriminal ecosystem

A cybercriminal ecosystem is composed of: all the individuals and groups involved in cybercriminality, their ways of working, and the processes they have adopted to maximize their profits while minimising their risks of legal consequences. Like all ecosystems, this is lively, dynamic, and undergoes permanent adaptation in order to exploit new opportunities in the marketplace, new vulnerabilities, new tools, and new means of communication.

This ecosystem is a part of, and inseparable from, the ecosystem of the digital society (Figure 10.2). It possesses its own specific structures while involving legal users of the Internet and benefiting from the services that these provide. This is notably the case of legitimate entities that provide the facilities for financial transactions, such as, to name only two, Western Union or Liberty Reserve.

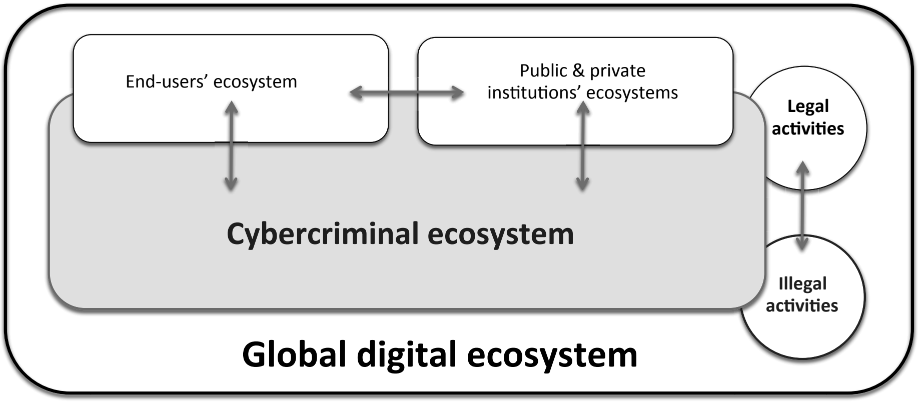


Figure 10.2 The global digital ecosystem.

The cybercriminal ecosystem benefits from all of the facilities provided by digital technologies and by the dematerialisation of transactions, from human weakness, and from problems on the technological, legal, and procedural fronts, whether these occur at a national or international level. This is made easier by:

- the existence of digital paradises;
- the fact that not all countries share the same political desire to combat cybercriminality, nor possess the organisational structures or resources to do so;
- the complexity and length of the procedures involved in international cooperation between police and legal systems;
- the way that digital traces can be mixed up, deleted or falsified. In addition, digital traces can be difficult to collect and interpret. Thus, it is not always possible to use these traces to identify criminals;
- the way that cybercrimes are increasingly committed using the combined skills of multiple individuals for specific tasks, often in separate and restricted contexts that are, taken in isolation, reasonably minor. These players convene for specific criminal projects of a fixed duration. They work together in virtual teams, dispersed around the world, based on their knowledge and skills, thus minimising their individual risk.

These cybercriminals demonstrate a great suppleness and flexibility, qualities that are not necessarily shared by the people and the structures engaged in the fight against cybercriminality.

The black markets of cybercriminality

Cybercriminals are rational beings who follow the laws of the market and of supply and demand. They are, above all, criminals who have learned to extend their activities, knowledge, and techniques into cyberspace. Just as there exists a black market and a hidden economy in the physical world, the same can be found in cyberspace. These cybercriminal black markets work in the same manner as classical markets, with the objectives of performance and profitability, feeding the whole chain of cybercriminality and relying on the communications tools and opportunities for contacts provided by the Internet.

These markets use the same mechanisms, knowledge, and tools as those activities linked to online advertising and legal e-commerce. They can be found at all stages of the performance of cybercrimes, of their preparation, and their monetisation. In addition, the Internet contributes in a major way to realising their profits. Among the different possibilities offered by the black markets, it is possible to:

- buy an on-line phishing kit, install it on a bulletproof server (classic hardware and software platforms), operate it (carry out phishing), collect the data gathered, and sell these through forums, on-line shops, and financial transaction services;
- buy and sell exploits, malware, and ransomware, software that allows cyberattacks to be carried out;
- rent zombie machines and create and operate botnets;
- buy and sell, wholesale or in small quantities, personal data, such as banking details.

The cybercriminal black markets are very much focused on the following needs (Figures 10.3 and 10.4):

- *Knowing the vulnerabilities* that can be exploited in carrying out attacks. The first to discover weaknesses and know how to exploit this for gain will always have a competitive advantage;
- *Possessing tools* to exploit these vulnerabilities;
- *Having access to individuals* willing to buy the tools necessary for committing cybercrimes (ICT or security specialists, good social engineers) and who are then prepared to plan and carry out the crimes (accomplices, intermediaries such as mules used for transferring funds, black hat hackers).

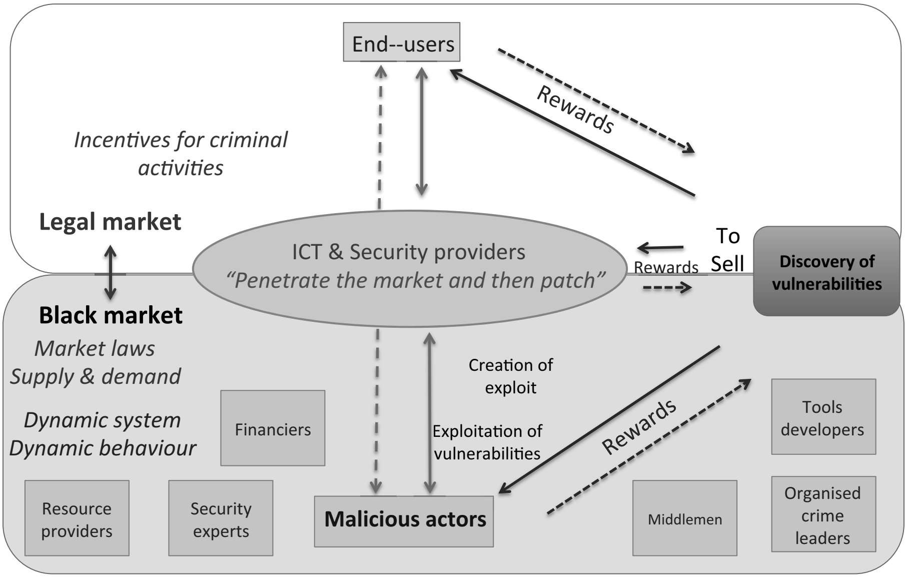


Figure 10.3 The cybercriminal black markets.

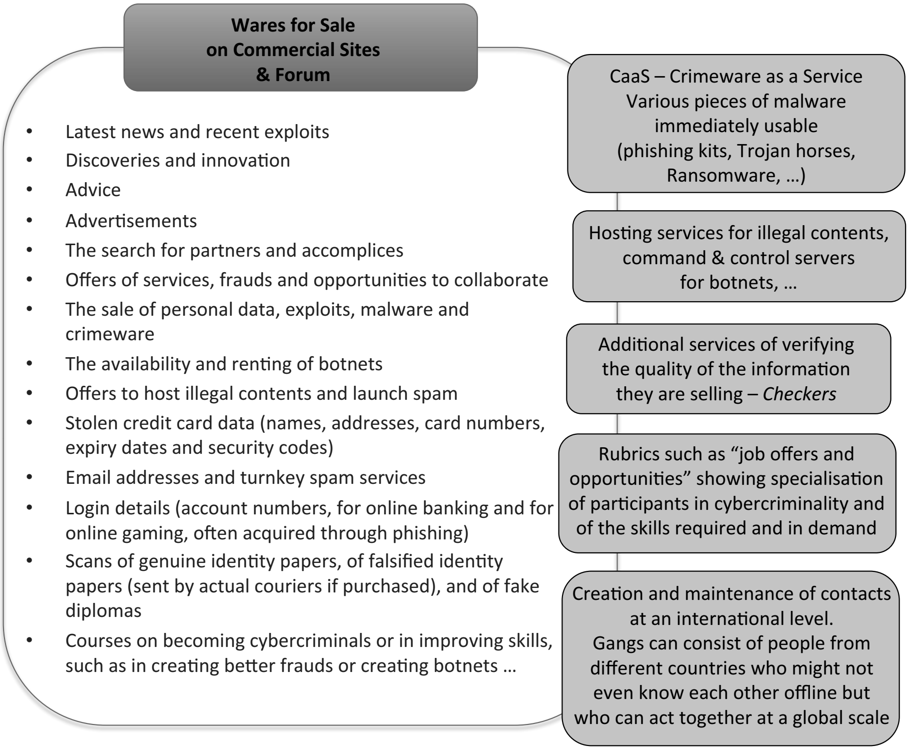

Wares for Sale
on Commercial Sites
& Forum
• Latest news and recent exploits
• Discoveries and innovation
• Advice
• Advertisements
• The search for partners and accomplices
• Offers of services, frauds and opportunities to collaborate
• The sale of personal data, exploits, malware and crimeware
• The availability and renting of botnets
• Offers to host illegal contents and launch spam
• Stolen credit card data (names, addresses, card numbers, expiry dates and security codes)
• Email addresses and turnkey spam services
• Login details (account numbers, for online banking and for online gaming, often acquired through phishing)
• Scans of genuine identity papers, of falsified identity papers (sent by actual couriers if purchased), and of fake diplomas
• Courses on becoming cybercriminals or in improving skills, such as in creating better frauds or creating botnets …
CaaS – Crimeware as a Service Various pieces of malware immediately usable (phishing kits, Trojan horses, Ransomware, …)
Hosting services for illegal contents, command & control servers for botnets, …
Additional services of verifying the quality of the information they are selling – Checkers
Rubrics such as "job offers and opportunities" showing specialisation of participants in cybercriminality and of the skills required and in demand
Creation and maintenance of contacts at an international level. Gangs can consist of people from different countries who might not even know each other offline but who can act together at a global scale

Figure 10.4 Black markets, e-commerce related activities, and communications services.

These black markets can know market fluctuations that are heavily driven by the lifecycle of vulnerabilities. Vulnerabilities that are not yet widely known, and for which no security patches yet exist, are the most difficult to identify but simultaneously the most profitable for those who exploit them. At the same time, the more that these weaknesses are exploited, or the more significant their impacts, the more likely it is that security countermeasures will be developed. The vulnerabilities, and consequently the exploits, become less profitable for the criminals, their value depreciates, and eventually, they become obsolete.

The cybercriminal ecosystem will remain in equilibrium for as long as those involved obtain profits significantly greater than the risks they run of being pursued by the forces of justice. This depends both on the real risks, which may or may not be well managed and controlled on the basis of the strategies adopted, and on the perception of these risks.

Between the maximisation of the wealth created through cybercriminality, the rapidity of the profits, and the risks of being arrested, certain cybercriminals have developed a real system of economic intelligence that is both dynamic and adaptable in the service of criminality.

10.2 The place of the struggle against cybercriminality in the cybercriminal ecosystem

When considering the cybercriminal ecosystem, it is essential not to forget everyone else who is concerned by it, that is to say the individuals and the organisations who, depending on the circumstances, can find themselves the targets of, or the willing or unwilling participants in, cybercriminal acts. This latter distinction can be illustrated, for example, by the way that users unwittingly become a link in a criminal chain as a result of fraud or manipulation. This is the case, for example, when a user's machine or an organisation's server acts as a relay or becomes a zombie member of a botnet used to carry out denial of service attacks on a third party. At the same time, a user can knowingly lend his machine to a botnet run by hacktivists, for example out of ideological, political, economic or religious convictions. Public and private organisations, completely legally, can also be led to use the same weapons as cybercriminals in order to defend their interests. This can occur in the context of both offensive and defensive cybersecurity. An additional point to consider is that whenever an organisation represents certain values prized by the cybercriminals, as is the case of banks or commercial organisations offering online services, or whenever an organisation is responsible for the creation of assets, services, software, or ICT or security solutions, that organisation by definition becomes a part of the cybercriminal ecosystem. Their presence in cyberspace, like that of Internet users who are very visible on social networks, for example, in some way explains the presence of cybercriminals and their activities.

The cybercriminal ecosystem would be incomplete if we did not include the police forces and judicial institutions that contribute in a concrete operational way to combatting cybercriminality (Figure 10.5). They run criminal investigations and can be led to create honey pots. They use the same technical knowledge and tools as the cybercriminals. They can draw upon the specific technical knowledge of specially trained officers, of external civilian experts, or even of genuine cybercriminals, who may have repented or who simply have no other choice but to collaborate with the police. They can apply both their technical skills and their knowledge of the criminal environment to become full partners of the police, or act as informers, or actively work to deceive other cybercriminals, or track criminal activities and unmask their perpetrators.

As with classical investigations, this work requires a real police skill-set, as it is not sufficient simply to be technically sound to be a good cybercrime investigator. They may have to operate undercover in order to infiltrate discussion forums on the black market, for example, or to infiltrate digital networks, which can be necessary in operations, for example, against Internet paedophiles.

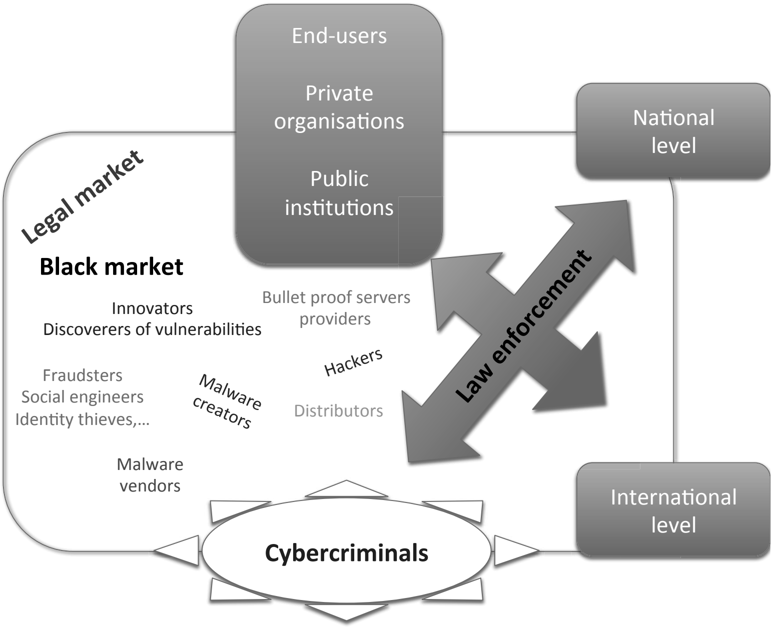


Figure 10.5 The Global cybercriminal ecosystem.

10.3 Cybercriminal investigation

A classical crime resolution process

Any criminal investigation follows procedures developed in a specific appropriate framework. Some variations will exist from country to country, but the following steps will usually be found: searching for indications and clues, identifying and localising the criminals, and presenting evidence to a court.

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 10.6).

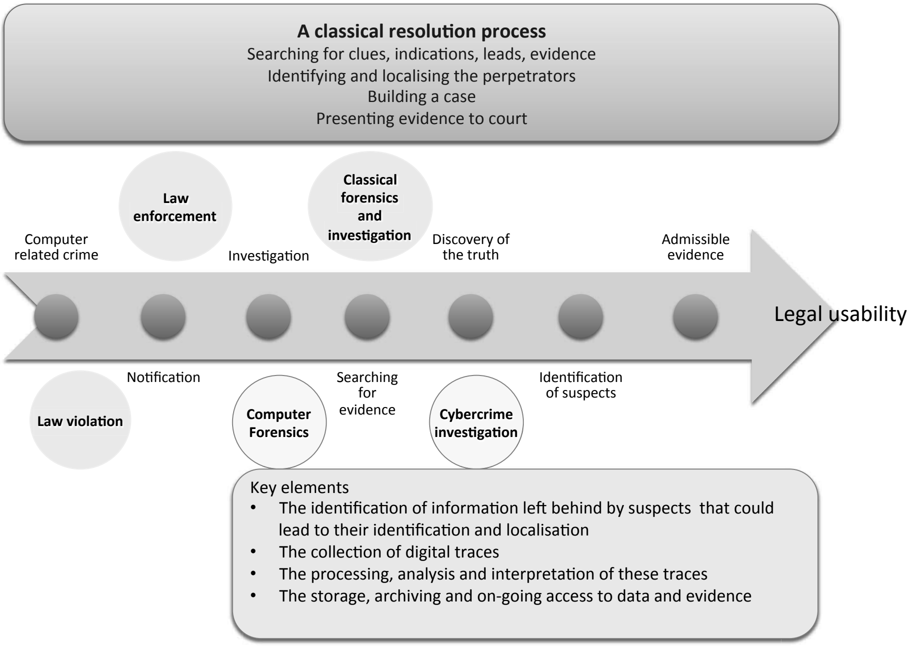

A classical resolution process
Searching for clues, indications, leads, evidence
Identifying and localising the perpetrators
Building a case
Presenting evidence to court
Law enforcement
Classical forensics and investigation
Computer related crime
Investigation
Discovery of the truth
Admissible evidence
Legal usability
Notification
Searching for evidence
Identification of suspects
Law violation
Computer Forensics
Cybercrime investigation
Key elements
The identification of information left behind by suspects that could lead to their identification and localisation
The collection of digital traces
The processing, analysis and interpretation of these traces
The storage, archiving and on-going access to data and evidence

Figure 10.6 Overview of a crime resolution process.

Keeping objectives and outcomes in mind

The reasons for conducting a computer investigation should not be forgotten. Moreover, 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; investigators must know the legal framework and constraints to perform a useful computer investigation. A good computer technician is not necessary a good ICT investigator.

Any computer systems information and communication device (electronic components, memory devices, hard discs, smartphone, game devices, USB sticks, etc.) or information it contains is a potential target for or instrument involved in the performance of crime. All devices can be the sources of digital evidence. Each piece of software, instance of processing of data, 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 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.

Both the kind of available information and its location in the system and network is mandatory knowledge for digital investigators. This means that they must understand how computers and networks function and are used.

To begin this process, an information-driven investigation must be executed by competent officers who have access to methodologies and tools that allow, among other elements:

- the identification of information left behind by misusers of information systems that could lead to their identification and localisation;
- the collection of digital traces;
- the processing, analysis, and interpretation of these traces; and
- the storage, archiving, and ongoing access to data and evidence.

10.4 The idea of digital evidence[1]

From digital traces to the identification of criminals: a difficult and complex process

Information presented in digital form and memorized by any electronic devices serves, if relevant and authentic, as evidence in a legal context. In a cybercrime investigation case, digital evidence can be even more difficult to obtain when it is scattered across systems located in different countries. In such a situation, success depends entirely on the effectiveness of international cooperation among legal authorities and the speed with which action is taken. Effective use of digital evidence to identify individuals depends on the speed with which requests are treated: if action is slow, identification is next to impossible. One of the most important features is the duration for which Internet Service Providers retain information concerning user subscriptions and activities (IP addresses, connection details, traffic 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 accord-

[1] This part is adapted from S. Ghernaouti-Hélie's publication:
"Information Security for Economic and Social Development." United Nations – Economic and Social Commission for Asia and the Pacific. 2007. Available at http://www.unescap.org/publications/detail.asp?id=1290

ing to national laws. 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 should be able to share critical information quickly, otherwise digital evidence may disappear, and cybercriminals will never be brought to court.

For Instant Messaging services and Peer-to-Peer or Internet Relay Chat facilities, logs and historical communications records are kept for only a few days, if indeed they are kept. In fact, there is no guarantee that logs or user records will exist or be conserved, or, if stored, with integrity. Digital traces can be rapidly removed from servers, and anyone can run an Internet Relay Chat server, for example, without further obligations.

Once the IP address of a system involved in a criminal activity has been identified, the next step is to determine who was using the system. It is always difficult to establish the identity of a person on the basis of an IP address, email, or web addresses, or a digital trace. A key question for law enforcement entities is how particular immaterial information can be linked to its physical author. An IP address identifies a computer, not a person; moreover, criminals use false or stolen identities to commit illegal acts (Figure 10.7).

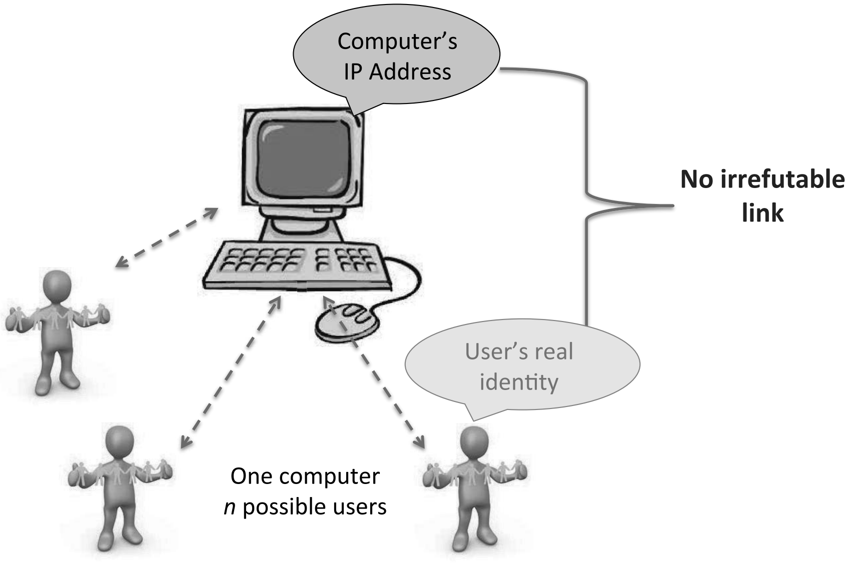


Figure 10.7 An IP address does not directly identify any individual person.

Furthermore, in most countries there is a significant mismatch between the skills of the criminals who commit high-technology crimes and the resources of the law enforcement and legal authorities to prosecute them. The use of computer technologies by these authorities, whether at the national or international level, varies greatly from one country to another but generally remains insufficient with regard to the amount of cases to be handled against the know-how and capabilities for adaptation demonstrated by the criminals. The lack of international regulations and control and, sometimes, the ineffective nature of international cooperation in legal investigations and prosecutions can allow cybercriminals to be quite effective. It is essential to possess procedures and effective tools that will allow the rapid localisation of criminals and permit rapid reactions on an international scale through efficient legal cooperation.

However, recently more and more countries are taking action to develop and maintain their cybercrime police forces and dedicate resources to international cooperation. For example, starting in 2014 Interpol will have an operational unit based in Singapore that is mainly dedicated to cybercrime.

From Interpol Global Complex for Innovation

Crime threats are changing
Police worldwide are facing an increasing challenging operational landscape, as criminals take advantage of new technology, the ease of international travel and the anonymous world of virtual business. Criminal phenomena are becoming more aggressive and elusive, notably in the areas of *cybercrime* and child sexual exploitation.

The future of policing
It is crucial for police to stay one step ahead of criminals. In today's world this can only be achieved if law enforcement officials have real-time access to information beyond their own borders. The digital age has opened up immense new opportunities to police forces, providing secure communications channels and instant access to criminal data. Innovation must become our best ally.

Championing innovation
The Global Complex will go beyond the traditional reactive law enforcement model. This new centre will provide proactive research into new areas and latest training techniques. The aim is to give police around the world both the tools and capabilities to confront the increasingly ingenious and sophisticated challenges posed by criminals.

The four main components of the Global Complex are as follows:

Innovation, research and digital security:
- Boosting cybersecurity and countering cybercrime;
- A forensic laboratory to support digital crime investigations;

- Research to test protocols, tools and services and to analyse trends of cyber-attacks;
- Development of practical solutions in collaboration with police, research laboratories, academia and the public and private sectors;
- Addressing issues such as Internet security governance.

Capacity building and training

- Research into training and methodology and the transfer of this research into police activities on the ground;
- Classroom, field and online training programmes for National Central Bureaus;
- Anti-corruption training, particularly in sport;
- Quality standards and accreditation.

Operational and investigative support

- Identifying and addressing emerging crime threats, for example, intellectual property crime, environmental crime and Asian Organized crime;
- A platform for disaster victim identification;
- A Command and Coordination Centre operations room;
- Incident response and major events support.

International partnerships and development

- Global partnerships with international organizations, governments, public and private sectors;
- Generation of revenue, donations and fundraising.

The Global Complex is being built in Singapore to complement our General Secretariat in Lyon, France, and to enhance the Organization's presence in Asia. The new Command and Coordination Centre operations room in Singapore will reinforce those already in place in Lyon and in Buenos Aires, Argentina. This presence in three continents will provide truly global operational support to our member countries […] The state-of-the art building will conform to the highest environmental standards and will become operational in 2014.[2]

About computer crime scenes

Before accessing a computer crime scene, police investigators and legal intermediaries must have received specific training. A common vocabulary between police forces, judicial officers, and technological laboratories should have been developed. Procedures and strict rules for data processing expertise should have been set up in order to increase the performance and reliability of computer investigations. The resulting investigation report should be easily

[2] http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation

comprehensible and must describe in detail both all the operations performed and the procedures followed to gather digital evidence.

Investigators with a solid understanding of information technologies and the Internet, who use cybercrime investigation methodologies in conjunction with effective international cooperation, should be able to uncover the identity of criminals. 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.

Searching for evidence

A trace is a mark, object, or sign not always visible to the naked eye, or a vestige of a presence or action at the place of the latter.[3] Whatever the nature of the trace, one must ask the following questions when investigating a crime (Figure 10.8): How was the trace made? Why is it present? Does its presence reveal an action that is relevant to the investigation?

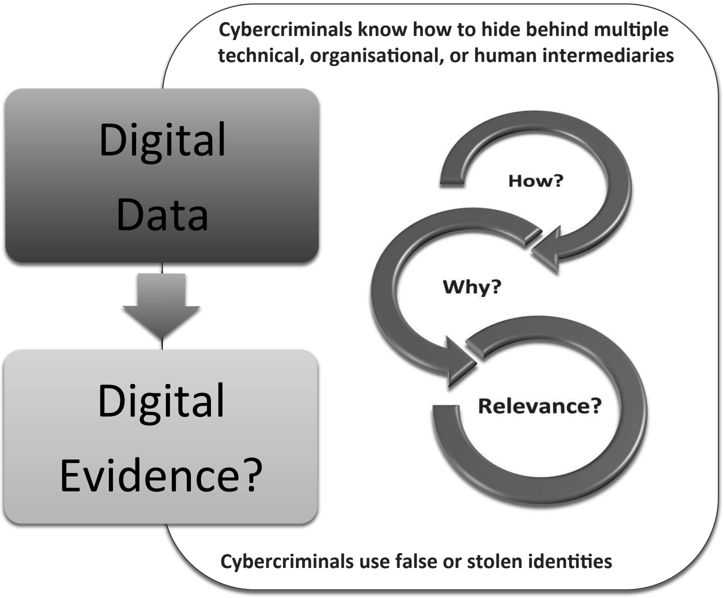

Cybercriminals know how to hide behind multiple technical, organisational, or human intermediaries
Digital Data
Digital Evidence?
How?
Why?
Relevance?
Cybercriminals use false or stolen identities

Figure 10.8 Some basic fundamental questions to be answered in a computer investigation.

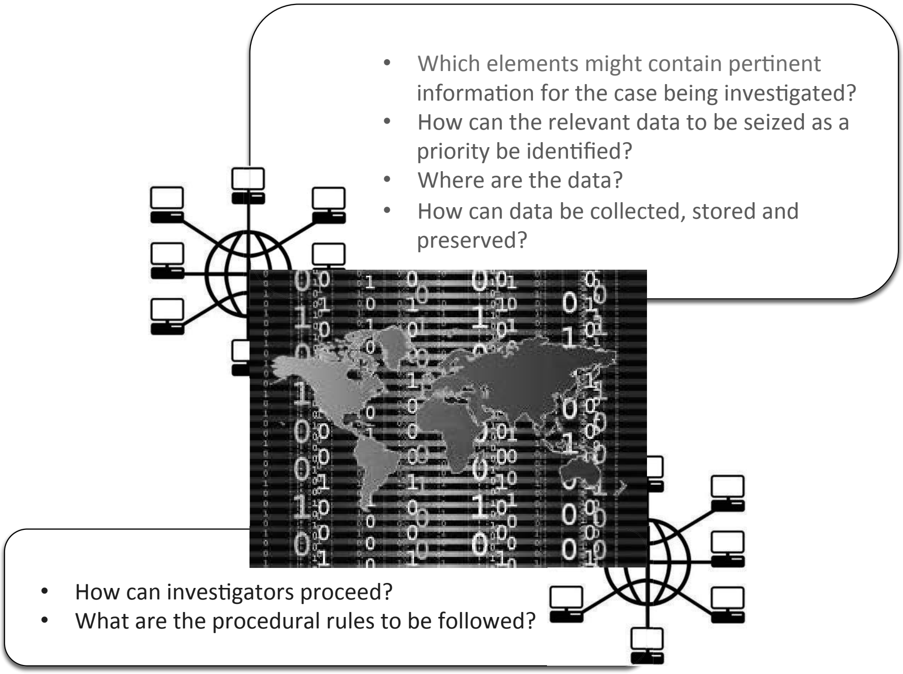
[3] Forensic Police Force, Reference Manual for the Federal Police Force professional examination, Switzerland.

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

When searching for digital evidence, many problems arise (Figure 10.9), including these key questions:

- Which elements may contain pertinent information for the case being investigated?
- How can the relevant data to be seized first be identified?
- How can investigators proceed?
- What procedural rules must be followed?
- How can data be collected, stored and preserved?
- How can data be safeguardeded and proof of its origins established, such that others may later analyze or review it?
- How can digital data be preserved as evidence for a potential trial, given that the storage medium from which the evidence was recovered is not infallible (for example, with date and time information being treated differently from one computer system to another) and subject to tampering?
- How can data be copied from its original support to another for analysis 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 data does or did not modify it?
- How can data copy analysis be conducted?
- How can deleted files 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 be linked to an individual?
- How can primary binary data be transformed into significant and comprehensible information?

- How can results be presented to non-specialists?
- How can one avoid digital evidence becoming a false alibi?



- Which elements might contain pertinent information for the case being investigated?
- How can the relevant data to be seized as a priority be identified?
- Where are the data?
- How can data be collected, stored and preserved?

- How can investigators proceed?
- What are the procedural rules to be followed?

Figure 10.9 Many sources of difficulties when searching for digital evidence.

To begin to answer these questions, some ICT computer forensic tools and procedures have been developed. However, only specially trained and competent experts should use them. Over the past few years, some evidence processing tools have been developed and commercialized, and their standardization is also a current issue.[4]

On the other hand, active communication monitoring and live surveillance could track criminals. Telephone, e-mail, or instant messaging eavesdropping is technically feasible to collect information related to both the content of communications and useful non-content, such as e-mail headers or IP addresses. In fact, criminals can also be identified through undercover investigation when investigators join, for example, Instant Messaging (IM) services, Peer-to-Peer networks (P2P), Internet Relay Chat servers (IRC), or newsgroups to lure

[4] Many digital forensic tools exist also in Open Source versions. See, for example:
http://www2.opensourceforensics.org/tools/paper
http://www.digitalforensicsassociation.org/opensource-tools/

criminals. But cybercriminals will always try to find ways to bypass security measures or to fool computer forensic tools or simply to develop anti-forensic actions. The following example shows how the community of file sharing has adopted new ways to download digital contents in a more secure way by using tools that ensure anonymity and uncensored file-sharing.

Most of the time the location of relevant digital evidence is not easily observable at first glance. We shall not forget that digital information is easy to damage, so information can be modified or destroyed such that it could no longer be used as evidence.

From the press

> *Anonymous, Decentralized and Uncensored File-Sharing is Booming*
> […] Faced with uncertainty and drastic changes at file-sharing sites, many users are searching for secure, private and uncensored file-sharing clients. Despite the image its name suggests, RetroShare is one such future-proof client. […] Anonymous, decentralized and uncensored are the key and most sought-after features. For some this means signing up with a VPN (Virtual Private Network) to make their BitTorrent sharing more private, but new clients are also generating interest. […] But there are more file-sharing tools that are specifically built to withstand outside attacks. Some even add anonymity into the mix. RetroShare is such a private and uncensored file-sharing client, and the developers have also noticed a significant boom in users recently. […] The RetroShare network allows people to create a private and encrypted file-sharing network. Users add friends by exchanging PGP certificates with people they trust. All the communication is encrypted using OpenSSL and files that are downloaded from strangers always go through a trusted friend. […] In other words, it's a true Darknet and virtually impossible to monitor by outsiders. […] RetroShare is about creating a private space on the Internet. A social collaboration network where you can share anything you want. A space that is free from the prying eyes of governments, corporations and advertisers. This is vitally important as our freedom on the Internet is under increasing threat," DrBob told TorrentFreak. […] "RetroShare is free from censorship: like Facebook banning 'obscene' breast-feeding photographs. A network that allows you to use any pseudonym, without insisting on knowing your real name. A network where you will not face the threat of jail, or being banned from entry into a country for an innocent tweet." In the long run this might drive more casual downloaders to legitimate alternatives, if these are available. Those who keep on sharing could move to smaller communities, darknets, and anonymous connections.[5]

[5] http://gizmodo.com/5890312/anonymous-decentralized-and-uncensored-file+sharing-is-booming?utm_medium=referral&utm_source=pulsenews, March 4, 2012.

10.5 Fundamental concepts in computer crime investigation[6]

The chain of custody

The chain of custody is an important concept when dealing with investigations, forensic science, evidence, and the application of law. It helps to preserve the integrity of evidence in order to avoid legal representatives of the defence successfully arguing that the evidence has been corrupted.

Like any item of traditional physical evidence, 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 how it has been handled (Figure 10.10).

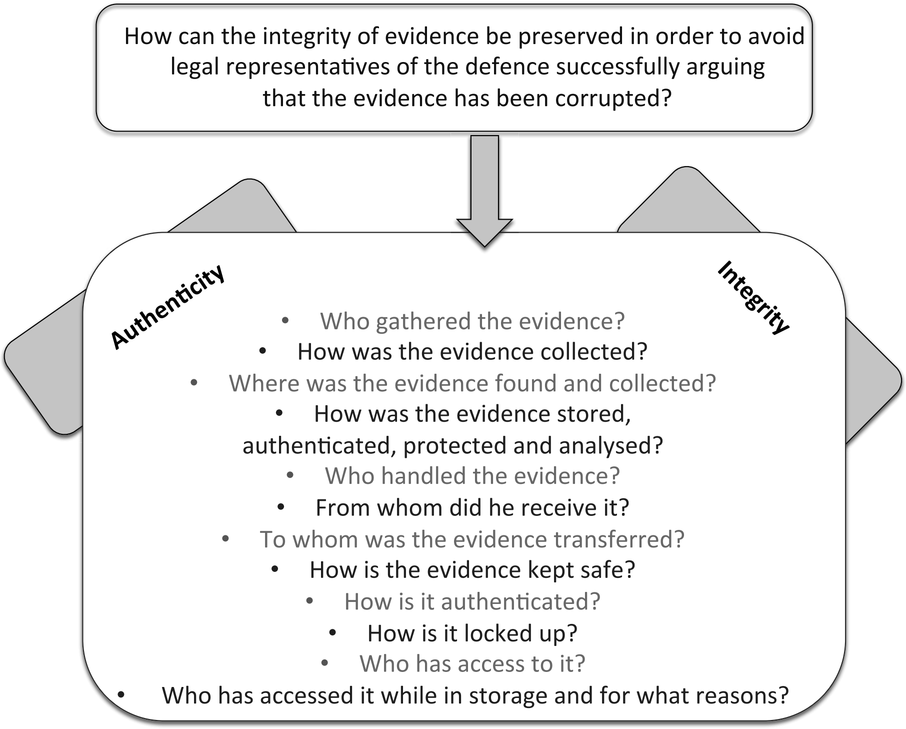

How can the integrity of evidence be preserved in order to avoid legal representatives of the defence successfully arguing that the evidence has been corrupted?
Authenticity
Integrity
• Who gathered the evidence?
• How was the evidence collected?
• Where was the evidence found and collected?
• How was 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 has accessed it while in storage and for what reasons?

Figure 10.10 Main requirements to be satisfied in a chain of custody.

[6] This part is adapted from S. Ghernaouti-Hélie's publication: "Information Security for Economic and Social Development." United Nations – Economic and social Commission for Asia and the Pacific. 2007. Available at http://www.unescap.org/publications/detail.asp?id=1290

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 collected?
- 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 has accessed it while in storage and for what reasons?

Computer crime investigation methodology

Just as criminals have developed attack methodologies and techniques that can help them to be efficient, investigators should optimize computer crime investigation by transferring practical knowledge into rigorous search strategies and methodologies and standard operating procedures (Figure 10.11). Before starting on a case, an investigator should carefully prepare his methods. Following specific methodologies is always beneficial and ensures that essential actions are not omitted in the pursuit of reliable and well-documented conclusions.

The aim of the preliminary phase is to gather information about the place and IT environment to be investigated (line of business, ICT resources and infrastructure, type of data, type 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 IT context from being modified before digital traces are collected, and to avoid giving the person or persons under investigation 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 as yellow tapes show the limits of a traditional crime scene. To prove the state of data at the time of intervention, data should be locked or 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

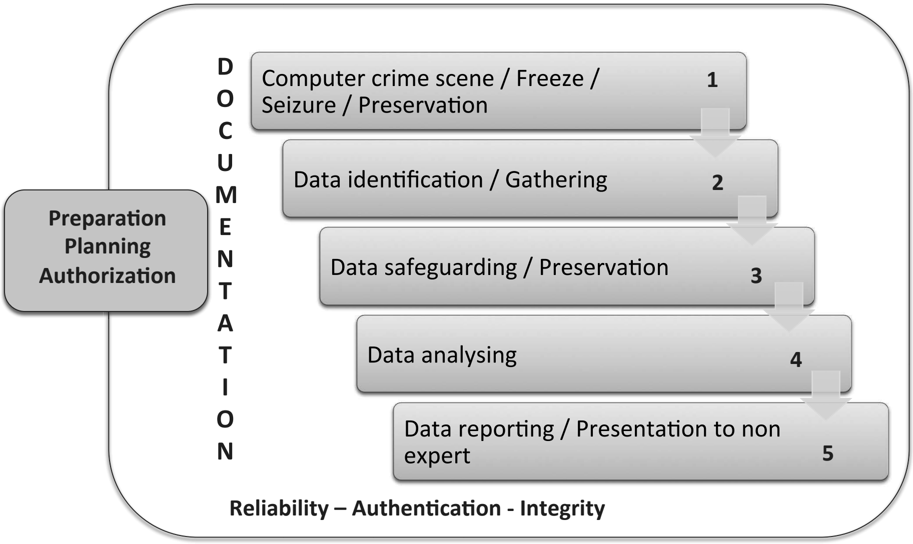

DOCUMENTATION
Preparation
Planning
Authorization
Computer crime scene / Freeze / Seizure / Preservation
1
Data identification / Gathering
2
Data safeguarding / Preservation
3
Data analysing
4
Data reporting / Presentation to non expert
5
Reliability – Authentication - Integrity

Figure 10.11 A methodology for investigating computer crime: basic principles and main steps.

investigator must classify resources to determine which systems or elements should 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).

Phase 2 consists of identifying traces and collecting them; 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 an understandable way for non-experts (Phase 5).

About digital forensics toolkits

A digital investigator should be able to call upon specialised technical tools for the collection, preservation, and analysis of digital traces, and then follow appropriately tailored procedures for the extraction and processing of data. This forms part of the overall methodologies for digital investigations (the idea of digital forensics), the end results of which should be the production of evidence that can be presented to and accepted by the courts.

All of this presupposes the following:

- that the investigator has the necessary technical background;
- that the data collected are an identical copy of the original data (no changes made to the data or the media);
- that the correspondence between the data presented and the original data can be demonstrated and authenticated;
- that in the case of storage media that have been damaged or destroyed, intentionally or otherwise, any data supposed to have been deleted or destroyed can be recovered in a useful form and condition; and
- that records of the time (time and date stamping) and the place of collection of data are systematically recorded, authenticated, and stored in a reliable way.

The data collected in this way should then be analysed, interpreted, and formatted in such a way that they are understandable to a non-technical audience that will include detectives, police officers, defence lawyers, magistrates, judges, and jury members. The investigators should always be capable of defending the results they have obtained, as well as describing and justifying the methods, tools, and techniques they have used to generate those results.

The majority of forensic tools available to investigators, be they commercial products or open source tools, offer the same kinds of functionalities, including:

- the creation of a bit-for-bit image – an exact copy – of the original data;
- the preservation of the data collected;
- time and date stamping;
- the recovery of files, directories, or data destroyed or hidden, and of the logs of actions or transactions;
- search based on a number of criteria (key words, types of access request, file types, types of programme, etc.);
- search for passwords;
- file descriptions (size, location, date of creation, date of last access, etc.)
- presentation of results; and
- possible analysis of encrypted files or of metadata.

These tools can be specific to the type of equipment, to the hardware, or to the operating system (smartphones, UNIX/Linux systems, Macs, PCs, etc.). Useful forensic analysis laboratories should have access to the widest possible range of forensic tools and operating environments and also to staff who are competent in the different technical environments they will encounter.

Examples of commercially available forensic tools

Encase Forensic by Guidance Software
EnCase® Forensic, the industry-standard computer investigation solution, is for forensic practitioners who need to conduct efficient, forensically sound data collection and investigations using a repeatable and defensible process. The proven, powerful, and trusted EnCase® Forensic solution, lets examiners acquire data from a wide variety of devices, unearth potential evidence with disk level forensic analysis, and craft comprehensive reports on their findings, all while maintaining the integrity of their evidence.[7]

FTK – Forensic Toolkit® by Accessdata
Forensic Toolkit® (FTK®) is recognized around the world as the standard in computer forensics software. This court-accepted digital investigations platform is built for speed, analytics and enterprise-class scalability. Known for its intuitive interface, email analysis, customizable data views and stability, FTK lays the framework for seamless expansion, so your computer forensics solution can grow with your organization's needs.[8]

Vogon Forensic Software by Vogon
Vogon Forensic Software comprises a range of imaging, processing and investigation software tools designed for the professional computer forensic investigator. The software has been developed by Vogon over the past decade to offer very high performance, extensive investigation facilities and comprehensive auditing and anti-repudiation techniques.[9]

Forensic E-mail Analysis Software: E-mail Examiner by Paraben
Forensically examine the most popular e-mail formats such as America Online (AOL), Outlook Exchange (PST), Eudora, and many others. Paraben's E-mail Examiner is one of the most comprehensive *forensically sound* e-mail examination tools available. E-mail Examiner quickly recovers deleted messages and folders. E-mail Examiner doesn't just recover e-mail in the deleted folders; it recovers e-mail deleted from deleted items (deleted/deleted). E-mail Examiner is just one component of P2 Commander, Paraben's comprehensive forensic analysis tool. This means advanced analysis features, easy bookmarking and reporting, advanced Boolean searching, searching within attachments, full Unicode language support, and a familiar and easy-to-use interface.[10]

[7] http://www.guidancesoftware.com/forensic.htm

[8] http://accessdata.com/products/computer-forensics/ftk

[9] http://www.vogon-investigation.com/evidential_systems-03.htm

[10] http://www.paraben.com/email-examiner.html

Example of an open source forensic tool

Live View developed by CERT, Software Engineering Institute

Live View is a Java-based graphical forensics tool that creates a VMware virtual machine out of a raw (dd-style) disk image or physical disk. This allows the forensic examiner to «boot up» the image or disk and gain an interactive, user-level perspective of the environment, all without modifying the underlying image or disk. Because all changes made to the disk are written to a separate file, the examiner can instantly revert all of his or her changes back to the original pristine state of the disk. The end result is that one need not create extra «throw away» copies of the disk or image to create the virtual machine.[11]

10.6 Investigating computer crimes within organizations

The general context

Committing computer crimes can have a variety of consequences for the functioning of organizations. Whatever form the crime takes, it can lead in various degrees to a loss of confidentiality, availability, reliability, integrity, know-how, credibility, and reputation, which individually or together can result in financial or even human damage. In a global economic context, such as the one that is emerging as the consequence of the globalization of economies, it is vital for many organizations to ensure the effective protection of their information systems.

Computer crime has today become commonplace. It takes various forms and affects different types of organizations. As a consequence, it is important to define the procedures to be implemented if one wishes to identify the perpetrators of such crimes.

To sufficiently protect itself, an organization should know how to set up the necessary structures. The first step is to define a coherent security policy in relation to the strategy and needs of the organization (Figure 10.12). This involves, in particular, an evaluation of the risks and cyberthreats that could potentially affect the activities of the organization. The management of this policy falls essentially within the responsibility of the ICT security manager. From an operational point of view, it results in the implementation of procedures, preventive tools, measures for the monitoring, control and audit of activities, and directives for reacting to and reporting on incidents and anomalies.

[11] http://liveview.sourceforge.net/

As a key part of the organization's management, the ICT security manager should participate actively in the evaluation of the information and computer related risks and in the definition of the security policy, as well as in the choice of the procedures and tools needed for its implementation and operation. He or she should manage daily activities at all levels – strategic, tactical, and operational – and ensure the control, validation, and updates of the security. He or she also has the duty of informing the senior management of the organization, a task that requires the regular production of summary and analytical reports. As is the case for every administrator, of course, the security manager will be subject to the traditional constraints of a financial, technological, human, and time-management nature.

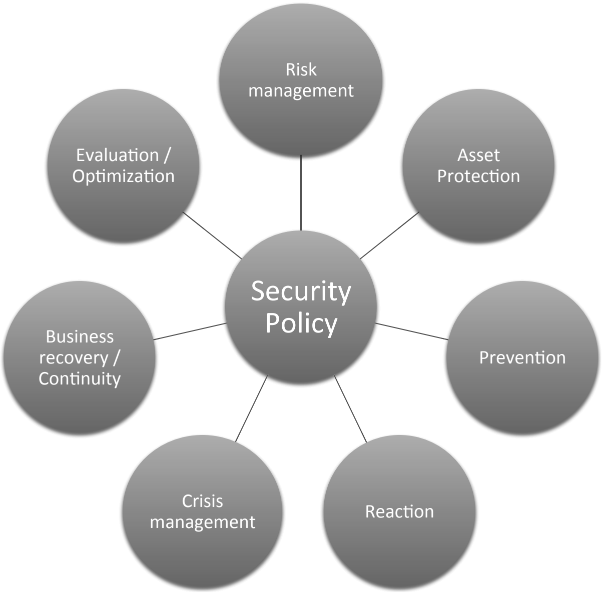


Figure 10.12 Main objectives of an ICT security policy within an organization.

Perspectives, constraints and potential obstacles

Problems with quality, a lack of know-how, numerous logistical constraints, and conflicting objectives are frequently at the origin of issues of mutual incomprehension between investigators and ICT security managers. There is a significant risk of seeing these differences become real obstacles to the proper performance of the investigation. While the security manager will have the objective of recovering and restoring key systems in the shortest possible time, so as to ensure the continuity of production, the investigator is subject to the formal constraints of legal procedure that require obtaining as many digital traces and potential sources of evidence as possible, and preserving them in accordance with precise legal standards. There is clearly a conflict with the instincts of the ICT security manager, which will be to stop any attacks on the systems and limit their consequences.

For the security manager, the problem of identifying the author is secondary to maintaining the organization's activities. To a certain extent, the recovery of the system represents, for him, the end of the incident, or at least of the reactive phase, although it is often situated at the beginning of the investigator's intervention (temporal gap). The procedures for rebooting information systems often conflict with the need to preserve traces of any attack, elements that would allow the nature and scale of the attack to be demonstrated, perhaps to identify a group of possible suspects, and to obtain legally valid evidence (Figure 10.13).

Furthermore, this gap can be widened by certain actions of a security manager or a system administrator if trying to solve the crime alone. Generally they possess only a partial knowledge of the legal constraints related to conducting a penal investigation, and usually they are not particularly experienced

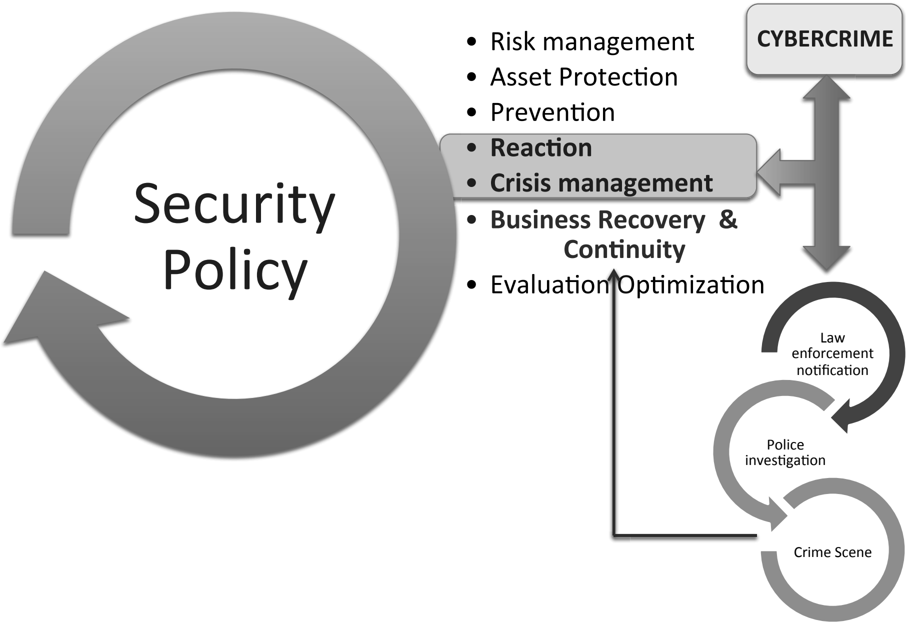


Figure 10.13 The relationship between ICT security policy and computer crime investigation.

in the correct management of traces. In addition, their attempts might have the effect of delaying police involvement, and, in many cases, they may attract the attention of the offender. Furthermore, they could be actively involved in the criminal activities. All of this will have the overall effect of slowing down, and even hindering, the progress of the investigation. At the same time, the investigator may be hindered by an insufficient vision of the technological, organizational, and human context of the concerned entity.

A certain number of obstacles to the smooth functioning of the investigation add to these causes of incomprehension. Such new forms of crime can lead, alongside the damage they cause directly, to an erosion of the image of the organization under attack, a consequence of which is the low level of reporting of such offences. Furthermore, the commonly perceived negative image of the technical skills of investigators increases the hesitation to report attacks. This perception of relative incompetence is strengthened by the police's lack of a communications strategy regarding these subjects. Viewed as insufficiently proactive, they do not succeed in using the cases brought to their knowledge as a basis for developing and communicating a more general framework of public policies dedicated to fighting cybercrime. This is why it is urgent to rethink the relationships between the police and information system managers, in order to effectively combat computers crimes.

Basic principles for effective cooperation

To be effective, the cooperation between the investigators and the ICT security manager must be based on a certain number of fundamental points. The various parties involved in the process all have to respect these basic principles.

Reducing the cultural and technological gap that separates policemen and ICT managers requires acknowledging the mandatory and inevitable character of their cooperation in the event of an investigation. This should permeate the understanding of objectives, with a particular emphasis on the importance of time constraints in managing their interactions. Specifically, it means that the human dimension of this relationship should be privileged. The technological aspect should remain a support for the action. This is why the implementation of idealised principles in a frequently uncontrollable reality will always require planning and preparation of the activities to be carried out, so that individual areas of action can be identified and attributed. The investigator will thus know where to perform and target the investigation, according to the information obtained at an early stage from the security manager responsible for the system in question.

The system manager clearly has a great motivation to follow these predefined procedures to effectively advance the progress of the investigation and resume control of the system as soon as possible.

In order to make their collaboration as effective and efficient as possible, the security manager should be able to supply the elements that will help the investigator in his work. For the most part, these will be drawn from the definition of the monitoring policy of the system, through specialized tools such as intrusion detection systems, and through the implementation of active audit procedures. It is also necessary to attend to the specifications of the backups and filing so as to improve the retention of high quality electronic traces. This particularly applies when the investigation is followed by a lawsuit. A judge will be all the more inclined to accept an electronic trace as valid evidence if this digital trace has been collected within the framework of the daily management of the system.

These elements are defined during the design and implementation of the information system. The arrival of an investigator at that point is unwelcome. However, after an incident has occurred, it can be useful to have additional information available that could accelerate the work of the investigator. First of all, it is essential to possess a complete inventory of the human, software, and hardware resources that make up the information systems. In particular, the configuration and location of the computer systems and the networks should be available, as well as a logical map of the information systems. Secondly, it makes good sense to use dedicated tools for collecting, storing, and analysing electronic traces; these tools should correspond to the requirements of a future investigation. This includes operational management tools for networks, means of performing traffic analysis, audit methodologies, intrusion detection systems, firewalls, and log files. The common use of rigorous procedures for the authentication of the data produced by all these means, in particular through controls over integrity and the time and date stamping of the relevant files, should enhance the value of the electronic traces that they preserve. In the long term, additional comfort can be provided by the regular copying of the most important data (logs of logins and errors, for example) onto read-only supports, such as CD-ROMs and DVD-ROMs. These various techniques and procedures will be of higher value in a legal context the more frequently they are undertaken and verified.

It is no longer possible to base a security policy on the principles of prevention and detection. This would only be effective if the criminals were consistently less competent than the system administrators. Nowadays, rather, it is mandatory to include, as early as the design phase of a security strategy, the elements needed for the effective cooperation between ICT security managers, and the investigators who would be in charge of identifying possible traces after an offence had been committed. To make this possible, two issues need to be addressed. First of all, it is necessary to create the conditions for real dialogue between representatives of two professional worlds who can frequently misunderstand each other. Secondly, the ways of designing information systems must be modified to permit, when the systems are live, the protection of the information generated by system management processes, so that this information could then be used in future judicial proceedings, if appropriate. What remains is to identify, or even create, the tools necessary for making the best use of the information that is created.

Among possible practical measures are the following examples:

- logs should be protected and authenticated;
- backup supports for log files should not be rewritable;
- the format of these files should be as universal as possible;
- the place where backups are stored should be protected;
- the duration of backup storage should be appropriately long;
- the risk analysis performed during the design phase of the security policy should lead to the definition of quantitative parameters allowing the evaluation of the critical nature of different log files;
- the security policy should be implemented and managed by skilled professionals; and
- these practical measures should from an integral part of the specifications of the security policy.

Collecting evidence in organization'scene of cybercrime

Basic recommandations

A cybercrime scene should be considered to be like any other crime scene with one added dimension, rather than as a completely different environment for investigation. The fundamental problem lies in the nature of the trace to be collected in distributed systems environments such as the Internet. The trace can be a “traditional” one, like a fingerprint, but it can also consist of information recording some action, for example, that the targeted system was not supposed to perform. When a network is used, these traces can be distributed over a number of interconnected systems. This introduces a new level of complexity into the daily work of an investigator who needs to determine quickly which traces are of the greatest importance and where to collect them. The first question is to know what to look for. Three types of evidence can be valuable:

- the evidence of the existence of the infringement;
- the trace of an action, or a transaction made through one of the systems in question; and
- a 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 potential evidence).

Challenges

The nature of the trace depends also on new criteria generated by the use of computer systems. In information technology environments, a trace is not necessarily the information by itself, but rather its digitized representation. Depending on how it is collected, a computer related trace could be considered as physical or not. For instance, if a log file is mirrored from the suspect's hard drive, it is a pure "non-physical" trace, while if the hard-drive is seized in order to use the log file as evidence, it is partly physical, since the support has to be treated as part of the trace.

Therefore, there is often a risk involved in the choice of which traces to look for in emergency and crisis situations, and of the first elements reported by the information system manager, who is usually the main interlocutor of the investigator. He or she has an obligation to promote business continuity that is not automatically compatible with the needs of an investigation. To complicate matters, that manager also could be implicated in the malevolent act and could have modified some traces to lead the investigator in the wrong direction.

The "human" dimension must necessarily be taken into account, since it could jam the communication between both parties. As Alphonse Bertillon[12] remarked: "One sees only what one looks at, and one looks at only what one has in mind." An investigator could be influenced by the traditional forensic way of exploring the scene of a crime. At the same time, a computer scientist or an information system manager will have a totally different perspective on the computer system and its environment. It is very important for the investigator to bear in mind the backgrounds and perceptions of those professionals when communicating with them.

The relative value of the traces that have been found must also be evaluated in light of the lifecycle of digital data. On a practical level, it is necessary to assess the value to an investigation or prosecution of traces in comparison to the technical difficulty and costs of obtaining and preserving them.

[12] A. Bertillon (1853-1914), French criminologist who created the first anthropometric system to identify individuals.

The notion of “legal usability” of a trace defines the ease of acceptance of the trace by a court. It implies the strong reliability of the processes for finding, collecting, and preserving the trace. In the case of a digital trace, it should also mean that it was created during the normal functioning of the system, rather than by a tool installed as a result of the incident under investigation and focused on identifying such elements. This notion can be linked to its technical counterpart “technical usability,” which is related to the level of specialisation required to understand and manage digital traces.

Traces localisation

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

It can be useful to classify the timings of potential digital traces in terms of the phases of the incident in question. This can give a breakdown as follows:

- Before the incident:
  - exploration traces (scans detected);
  - “normal state” of the targeted system (traces created by normal activity)
  - logs of firewall and intrusion detection systems.

- During the incident:
  - logs of the systems that could have been used, or targeted, by the attacker;
  - content of the swap files;
  - dump of system memory (RAM);
  - system process management.

- After the incident:
  - attempts at data modification, deletion or erasure (“cleaning” traces or creating false traces);
  - logs of current activity of the targeted system (can reveal rogue processes);
  - logs of connections from the attacker’s Internet Access / Service Point;
  - the attackers making themselves known: claims (on Internet Relay Chat, forums, etc.), blackmail (anonymous mail…).

The ability to perform this kind of time-based analysis will depend on various system management policies. Each policy has to be understood by the investigator when finding if a trace could still be collected somewhere in the system.

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

To reach this location, even from inside the enterprise, a criminal will necessarily use the infrastructure provided by an Internet Access Provider. The physical supports for the access provided could be different for each provider, and each one of them should have its own policy for the creation and retention of connection logs.

There are a number of places in which location information could be stored, depending on the precise circumstances of the incident:

- A 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, such as, for example:
  - intrusion detection systems;
  - firewall logs;
  - DHCP (Dynamic Host Configuration Protocol) servers;
  - authentication servers;
  - network load management tools; and
  - application servers (that could have been used during the performance of the crime);
- Internet environment investigation particularities: some of the "global carriers" (such as backbone operators) log a great deal of management information in order to better manage their quality of service. This also can provide clues about the attacker, or about the attacker's motivation.
- Internet Access or Service Provider (IAP/ISP): Network management tools used by the victim's IAP/ISP can be invaluable in finding the origin of the attack (the "attacking system") and the possible destination of some of the stolen assets (specific data or financial transactions);
- At the same time, the IAP of the attacking system can provide information about
  - the time of internet access (when done through ISDN or dial-up);
  - the amount of data exchanged, and sometimes when the connection happened (on permanent connections such as ADSL or cable), although this does depend on the existence of use monitoring logs;

- logs of incidents;
- details about which web pages (or sites) have been accessed, and when a proxy is used and configured, to keep a track of when the stored data have been retrieved.

The life cycle of a trace

In the forensics field, the lifecycle of a trace is particularly important if one wants to avoid its contamination or destruction. By way of analogy, investigators are used to handling biological traces in emergency, since most of these are often usable during only a short period. In cyberspace, evidence can be also 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 ease of creation*: this factor determines the technical difficulty encountered in creating the trace during the normal operations of the system. It has a direct effect on the legal value of the trace, since a malicious user could create a false trace, or alter a real one, where this is technically feasible;
- *The durability of the trace on the support*: this criterion helps to define which kind of support should be the object of the first investigations. The investigator must search urgently on the media that are the most volatile;
- *The speed of deletion by existing system tools*: usually, the deletion of a file is easily performed by the operating system. But some applications (such as database management systems or journaled file systems) automatically clear all or part of the data. 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 trigger conditions data are deleted by the normal activity of the system.
- *The ability to be fully erased*: some physical supports are very difficult to erase completely. Some 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 can still be recoverable after an incident.

New way of tracking evidence

Developing new ways of tracking evidence of cybercriminal offences is becoming mandatory, in the same the way as measures imposed to handle financial crime in the eighties. At that time, the appearance of new and complex financial tools, alongside the globalisation of the markets, led to a growth of sophisticated financial crime. A considerable effort was expended in teaching judges and police officers how to investigate such affairs. Once seen as “exotic,” financial crime is now fully integrated into judicial mechanisms, and even if its investigations need expertise, time, and means, it is no longer considered exceptional. In the same way, cybercrime is becoming more common, and the judicial system should handle it more easily as more and more investigators and judges are taught how to deal with it and its specific elements and contexts.

To accelerate this evolution, methods are developed to better classify incidents and help the investigators employ sufficient resources where 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 focused on the collaboration between the investigator and the people in charge of IT infrastructures and security affected by the offence. This can be improved specifically by the perception of the investigator as “computer literate,” or technically competent, by the system administrators. Two ways can lead to such professional recognition: education and formalisation. Education 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 investigators, researchers should develop a common method of cybercrime scene investigation that could improve both the efficiency of investigators and their acceptance by IT professionals.

10.7 Summary

Legal action against cybercriminals assumes that the malicious act has been identified and reported to the competent authorities and that these authorities are capable of carrying out their work. This requires an understanding of the criminal ecosystem, of the means, methods, and knowledge of the cybercriminals, and of their tools. When IT equipment becomes the object of the search for information, and starts to become recognised as similar to classical crime scenes, the investigators need either to be real specialists in information systems and security or to be able to call upon forensic experts. These experts will follow pre-defined procedures and will use tools appropriate for the circumstances of the crime. The identification and solving of crimes is based upon the analysis of smartphones, computers, and all types of electronic equipment used by the victims or the suspects; this analysis requires expert skills in computer forensics that, in turn, rely upon the facilities offered by actual forensic analytical laboratories.

10.8 Exercises

1. What is digital evidence?
2. Why is it difficult to identify an individual through digital traces?
3. Can a digital trace be considered as proof of guilt?
4. What are the limitations and difficulties connected to the identification and collection of digital traces?
5. Where can digital traces be found?
6. What kinds of digital traces do investigators look for first, and why?
7. What is an IP address?
8. Is it possible to identify an individual from an IP address?
9. Is it possible to be certain of having identified an individual based on (i) an email address or (ii) an IP address?
10. Define the idea of the chain of custody, setting out its end results and how it adds value to a criminal investigation.
11. What is the fundamental constraint to bear in mind when gathering digital traces?
12. What kind of skills and experiences should an IT investigator possess?
13. Define the notion of *retention period*.

Chapter 11

A Global Approach to Cybersecurity

11.1 Understanding the context

Meanings and interpretations

Several terms and interpretations are associated with the concept of cybersecurity. However, whichever name is given, be it information and communication technologies security (ICT security), information security, digital security, or Internet security, the central element remains: the security of digital information (Figure 11.1).

Information security is an answer to the risks associated with the use of information and communication technologies (ICT) in everyday activities. The objective of information security is to minimize informational risk and bring it under control; that is, to reduce it to an acceptable level.

Basically, security is:

- making safe or safer;
- the act of functioning without disorder or major difficulty;
- being protected from danger and countering risks;
- an ability to ensure the security of goods and people.

Cybersecurity refers to information security issues for governments, organizations, and individuals dealing with ICT technologies, and in particular with Internet technologies.

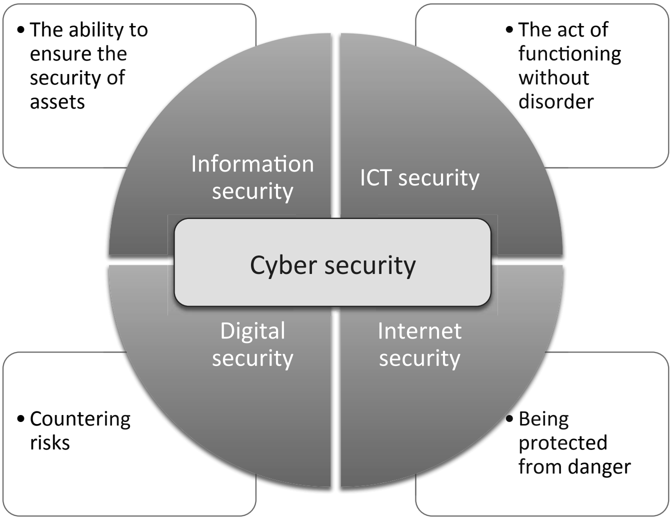

• The ability to ensure the security of assets
• The act of functioning without disorder
Information security
ICT security
Cyber security
Digital security
Internet security
• Countering risks
• Being protected from danger

Figure 11.1 Information security related concept.

Cybersecurity must insist on the strategic dimension of ICT infrastructure and services in respect of state sovereignty, organizational competitiveness, and the safety of individuals.

Cybersecurity cannot be abstracted away from its field of application and socio-cultural environment. It must be approached in an interdisciplinary and multi-stakeholder context, placing the individual at the heart of the ICT security question in order to encourage the development of a conscious and inclusive information society.

The terms "information security" and "cybersecurity" can carry different meanings. In some contexts it refers to the protection of assets or to the fight against industrial and economic espionage, against international terrorism or economic crime, against the manipulation of illicit contents or the unauthorized use of resources. In other contexts, cybersecurity covers everything from computer surveillance and monitoring to tyrannical control or to a struggle for fundamental human rights.

Information security deals with a range of issues, such as state sovereignty, national security, the protection of critical infrastructures, the security of tangible and intangible assets, and the protection of personal data, to mention only a few. In addition, any potential malfunction of information technologies, regardless of its origin (accident, error, malevolence), constitutes an operational risk for people or organizations that rely upon ICT, as they mean a consequent risk of losses from the inadequacy or failure of processes.

Of late, information security also includes topics related to cybercrime issues and to potential misuse of ICT or security. But cybersecurity also is arises from the need for technologies to be less vulnerable – to decrease the number of potential threats. Cybersecurity concerns the creation of secure, transparent and manageable products, the development of reliable and safe behaviours around the use of ICT, and the definition of appropriate legal frameworks. Because humans are the weak link in the security chain, and because humans are the final "consumers" of ICT service and infrastructures, any security solution should also take into consideration social needs. At the same time, security solutions should not transform the Internet and information technologies into an excessively controlled territory, because their doing so may undermine basic human rights.

At the crossroads of technological, legal, sociological, economic, and political fields, IT security is interdisciplinary by nature. It must not only reflect its location, depending on the country, and that nation's values, culture, and civilization, but also meet the specific security needs of the local context (Figure 11.2).

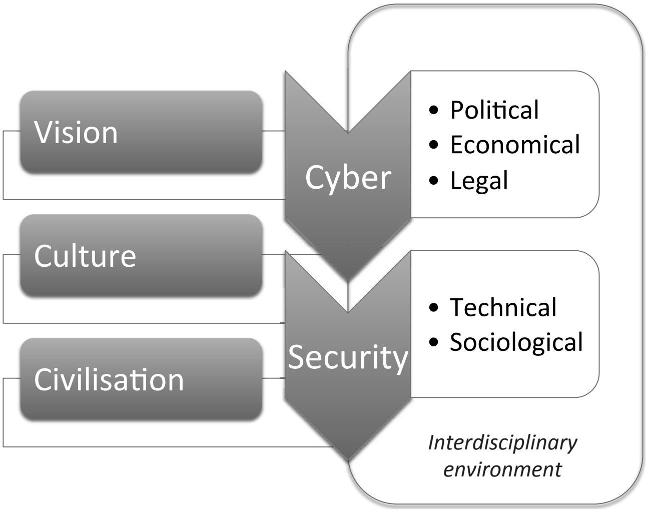


Figure 11.2 The security concept is context dependant.

11.2 The evolution of information security

Information security has always existed, but historically it was only of interest to specialists, and, until the middle of the 1990s, cybersecurity was viewed as a technological issue (Phase 1) to be addressed by engineers (Figure 11.3).

The first operating system (OS) already included access control mechanisms and cryptography, which was mainly reserved for critical applications in sensitive domains such as the military, banking, and general finance. Network security was an integral part of network management, alongside configuration management and performance monitoring. Since then, the limits of a purely technological approach, one that uses security tools in a non-integrated and incoherent way have been identified (for example, applying at different times security measures designed to address separate needs and issues, the inconsistent application of patches and updates). A managerial approach to security then emerged that addressed the need for a global and consistent treatment of security requirements. In particular, this manifested itself in the development of standards for security management, such as the ISO 17799 and ISO 27000 families. While evolving from a technical field to a management field, the IT security concept gave way to technological and informational risk management (Phase 2).

However, security management cannot overcome failures resulting from design problems or the criminal misuse of ICT infrastructures. Illegal eavesdropping, system intrusions, the propagation of malware, the exploiting of vulnerabilities; all of these activities are showing continuous growth. Information security concerns the organization regarding the protection and defence of assets by taking into account the intrinsic vulnerability of information technologies and the criminal threats to the strategies of organizations.

As technology and management do not make it possible to completely avoid incidents, and “zero risk” does not exist, responsibility issues have become central with regard to information security. This has contributed to moving the borders of management security out towards legislation (Phase 3). Security solutions can protect a given environment in a particular context, but cannot prevent criminal behaviour altogether. Legal institutions and laws should exist to dissuade criminal behaviour and to bring to justice people who carry out illegal acts.

Because ICT security is a major concern for governmental, diplomacy, and military issues, the political dimension completes the technical, managerial, and legal approaches of information security (Phase 4). Cybersecurity also concerns state sovereignty, national security, and the safety of citizens. In a broader sense, it includes the protection of consumers, the protection of children, and the protection of civil liberties and democracy.

There are many ways for malicious people to exploit vulnerabilities. The list of these types of attacks or methods is long, and the techniques are in constant evolution. These include, for example: identity theft, system spoofing,

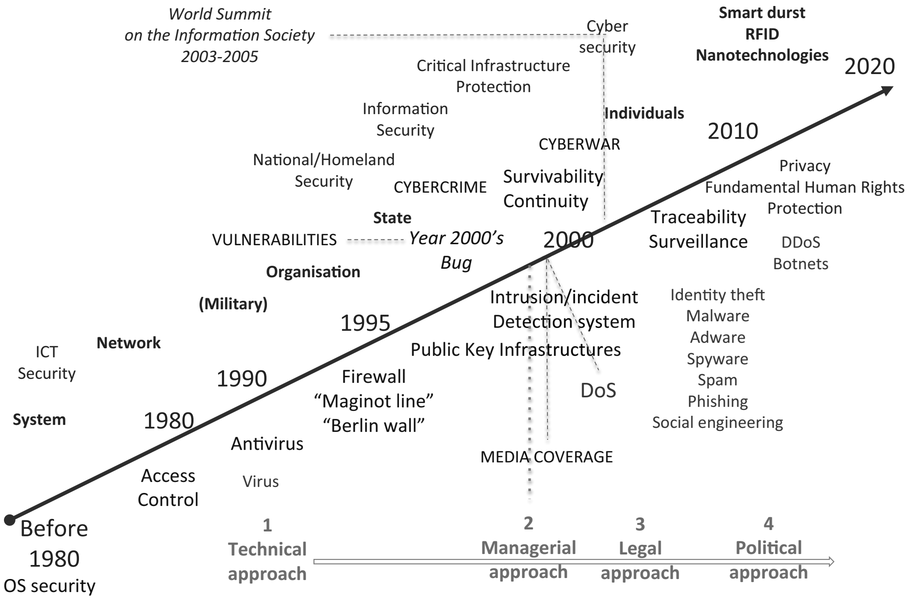


Figure 11.3 ICT security evolution.

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. At the same time, however, the global Internet is relatively robust. At the time of writing, there have not been disastrous global cyberattacks with critical impacts on infrastructure and services. In any case, regardless of criminals' motivations, the results always include a significant economic impact. Cybercrime is fast turning into an international hydra, a multiple-headed monster.

As information is one of the most important values of the information society, the protection and defence of that information is crucial.

Cybersecurity is essential to the success of Internet for the use of states, organizations, and citizens.

The Internet has become a necessity of the information society. It can 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 the technologies and services provided by the Internet. The concept of criticality associated with information or, more generally, with infrastructures, relies upon its level of importance and determines the survival of those who depend on it. However, the ICT infrastructures belong only partially to those who depend on them. Even the so-called "public-Internet" infrastructures" belong, to a large extent, to private companies. In this context of dependence and interdependence on telecommunications and on electrical infrastructures, the cybersecurity dimension is of prime importance.

A trend is emerging in terms of the understanding of Internet security. This tendency is towards a less well-defined but more complex terminology relating to the protection of critical information infrastructures. This modification of terminology without clear and standardised definitions introduces more complexity, and could lead to an overemphasis on cybersecurity in the protection of critical information infrastructures and homeland security.

ICT security raises a lot of still-open questions that go beyond the purely technological dimension of Internet and its security. Cybersecurity should cover everyone, and it should extend protection to personal data.

The currents limits

Statement 1

Historically, security was handled only in its technological dimension, before other aspects, such as the managerial or legal dimensions, were taken into consideration. While this evolution was principally good, these additional dimensions have frequently been taken into account independently rather than as part of a systematic and multidisciplinary approach. This shows how the perception of the security issue can change without necessarily leading to a resolution of the issue.

Inefficient, inoperable, and sometimes conflicting solutions could, therefore, be the result of a non- integrative approach. The consequence is that this often introduces new weaknesses and vulnerabilities in shifting the responsibility of security onto other actors or entities, and it produces a false sense of security.

Security solutions exist but cannot be all-encompassing. Good security policies allow, as far as possible, the management of ICT-related risks, which reduces the probability that they will arise. More often, ICT security strategy is often limited to a purely technological approach of setting up mechanisms to reduce the risks to the organization's information assets.

However, even though a good security manager will be able to anticipate or prevent certain voluntary or deliberate accidents, not everything is predictable. In addition, there is usually more talk in security circles of data than of human integrity. No security service, however sophisticated it might be, focuses on the integrity of network administrators or users. The weakest link in security is human.

Statement 2

In general, security solutions exist but are inefficient because:

- most people involved think only about the tools, not about tools, process and management;
- tools are not effective and flexible enough;
- tools offer a static and specific answer to a dynamic and global problem;
- international security standards or recommendations exist but are not necessarily implemented;
- there is a lack of training and skills;
- legal provisions have been specified by people who sometimes do not fully integrate the user's point of view into the technological, managerial, or economic issues (mainly because it is too complex);
- the design and distribution of ICT products do not place sufficient importance on security;
- there is no clear sharing of responsibility between technical intermediaries, ICT, and security providers, so it is easier to shift the responsibility for security to the end user;
- no one wants to bear the cost of security;
- often, security is synonymous with obscurity, i.e., there are tools for ensuring the transparency and efficiency of controls for technical security solutions or security management.

Statement 3

As the Internet has grown, so has connectivity, enabling attackers to break into an increasing number of systems. This is often possible because non-secure, non-robust systems are used and many of these cannot resist a determined attack if they are not well protected and monitored. Attack tools are widely available to the general public. Security solutions or patches are not always implemented. Management procedures and controls for system configuration and administration are defective. Human weaknesses are a reality. Existing security technologies are fallible or could be circumvented. Moreover, it is difficult to define and support an effective security management process alongside a global, dynamic, and consistent security approach. In this context, individual, organizations, and states must be aware of new sources of vulnerabilities and threats introduced by ICT use and dependency.

Statement 4

Criminality and deliberate errors are not the only sources of insecurity on the Internet. Various problems in the design, management, and use of systems can provoke security incidents. The hardware, software, and environmental infrastructure of the Internet can break down as a result of natural catastrophes (fire, earthquake, flood) or of mistakes. Failures, malfunctions, errors, mistakes, inconsistencies, and even natural disasters generate cyber insecurity.

The use of the Internet for business and social activities 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. This 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, accessibility, and the respect of fundamental human rights. As previously stated, costs must be realistic and managed. Third, e-services should be reliable and trustworthy; the security criteria of integrity, confidentiality, authenticity, and availability have to be guaranteed. Furthermore, traceability and proof must be possible for activities under third party control. Security and trust are relative notions, but they are both critical factors of success and business enablers for any e-economy. The underlying problem is found at the level of security and confidence offered and guaranteed by information and communication technologies providers. This could be summed up by the question: "Who is in control of the infrastructures, access, use, services, content, and security?" Fourth, an enforceable legal framework should exist, and criminal laws should be updated to adequately cover the extensive use of data processing and telecommunications. Procedural standards should be defined to allow governments access to stored or transmitted data, where appropriate, while respecting privacy protection, civil liberties, and public safety. 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.

11.3 Avoiding the cybersecurity gap

Beyond the inherent limits of security technologies

Focusing more on information systems and network security, the following elements from the Organization for Economic Co-operation and Development's (OECD) 2002 guidelines for the security of information systems and networks – "Towards a Culture of Security"[1] – are a good starting point for examining security issues. Although published a decade ago, they remain a robust set of general guidelines that can be applied independently of technological developments.

- *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;
- *Response*: participants should act in a timely and co-operative 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 basic 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.

These security guidelines apply everywhere and constitute a good starting point for considering ICT security issues. They can be integrated and summarized in a diagram of a security architecture concept (Figure 11.4).

ICT security is not simply a cultural problem that has a technological dimension. It is also a regulatory issue. A cyberspace regulatory framework could help to transform the Internet into a safer place to conduct activities. An appropriately adapted legal framework and laws that are applicable to the digital world must be both operational at the national level and internationally compatible. At the same time, qualified participants in the justice system and police authorities skilled in ICT and cybercrime should enforce the legal aspects of information technologies and cooperate with their partners at the international level.

The need to integrate a legal dimension relating to data processing is increasingly being felt by organizations. This relates, for example, to data conservation, the responsibilities of technical staff, the management of personal

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

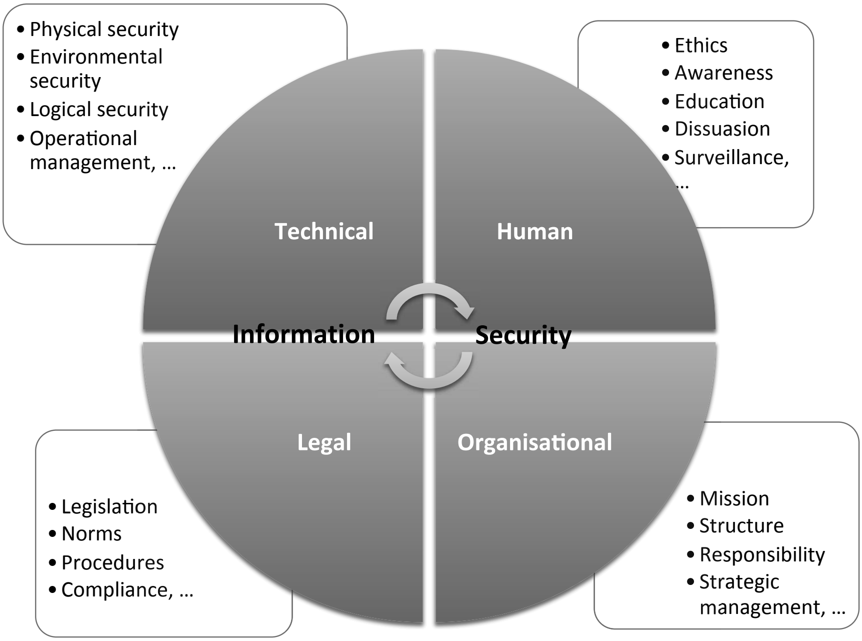


Figure 11.4 An information security architecture concept.

data, the cybermonitoring of employees, intellectual property, IT contracts, and e-commerce, to name just a few aspects of business management, and regulatory compliance.

The legal conformity of information systems is a new dimension that will need to be taken into account by the officers in charge of information system and data processing. Thorough knowledge of new technology-related laws is becoming a necessity, and the law must be borne in mind when installing security solutions. Legislation becomes an endogenous factor when considering security and can be seen as a security driver.

The omnipresence of legislation in information systems governance can become a strategic asset for organizations, as legal intelligence constitutes a key factor of success for corporate strategies. Thus, the staff in charge of security for organizations should also be made aware of the constraints of police investigation (minimal documentation relating to incidents, conservation of logs, etc.). These measures only make sense when incidents are reported to the police.

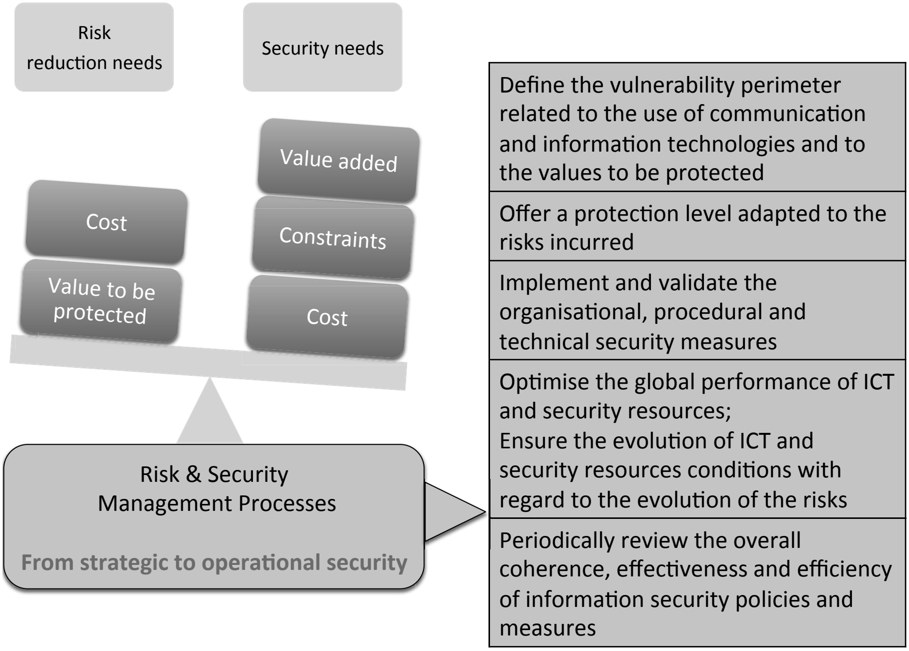
At a national level, countries must support the reporting of cybercrimes and work to build confidence among the various participants in the economic world, the justice system, and the police.

In order to meet the need for monitoring and reaction, auditing mechanisms should be designed and implemented in and around critical systems. These mechanisms should report violations of a defined policy or report actions that are considered to be security threats.

The use of strong identification and authentication solutions, operational cryptographic mechanisms, and one-time passwords are strongly recommended to enforce network security. Automated or semiautomatic techniques for guiding the selection of mechanisms for enforcing security policies and rules previously defined must also be envisaged.

Security can be improved by, for example: (Figure 11.5):

- understanding better ICT related risks;
- finding the right compromise between risk reduction and security needs;
- knowing and monitoring vulnerabilities and security solutions;
- fixing computer and network security flaws;
- avoiding single points of failure;
- efficient network management, identity management, and access control solutions;
- efficient information security and quality management;
- adaptability in defensive activities.



Define the vulnerability perimeter related to the use of communication and information technologies and to the values to be protected

Offer a protection level adapted to the risks incurred

Implement and validate the organisational, procedural and technical security measures

Optimise the global performance of ICT and security resources;
Ensure the evolution of ICT and security resources conditions with regard to the evolution of the risks

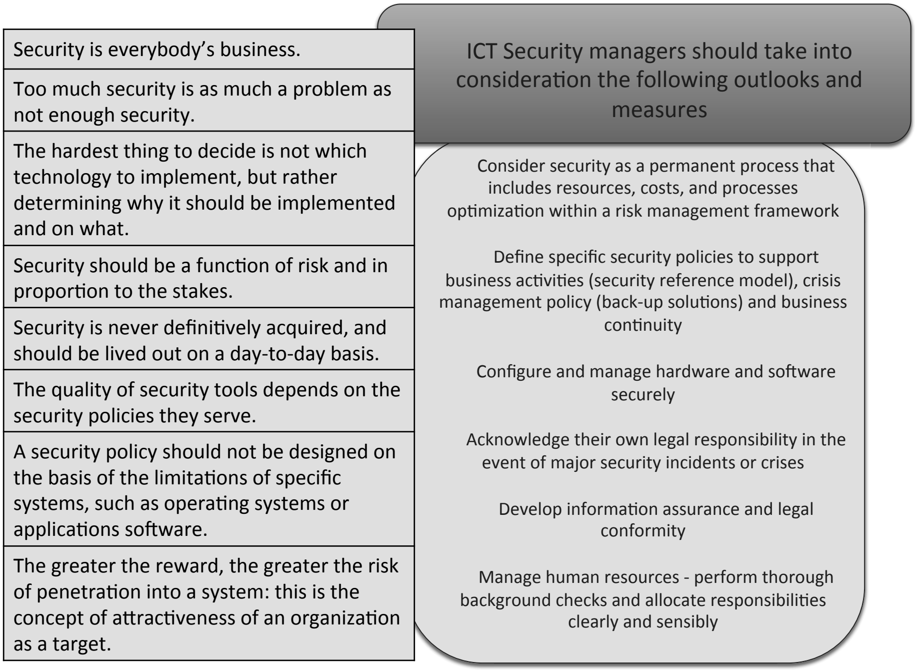
Periodically review the overall coherence, effectiveness and efficiency of information security policies and measures

Figure 11.5 Some contributions to improving the overall ICT security level.

At the same time, information technology managers have to:

- consider security as a permanent process that includes resources, costs, and process optimization within a risk management framework;
- define specific security policies to support business activities (security reference model), crisis management policy (back-up solutions) and business continuity,
- configure and manage hardware and software securely;
- be aware of their own legal responsibility in cases of major security incidents or crisis;
- develop information assurance and legal conformity;
- manage human resources (check personal background, define responsibilities, educate, etc.).

Without the will to integrate all components of a security system using a systemic approach, security solutions will not sufficiently protect a distributed and ever increasingly mobile IT infrastructure (Figure 11.6).



Security is everybody's business.

Too much security is as much a problem as not enough security.

The hardest thing to decide is not which technology to implement, but rather determining 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, such as operating systems or applications software.

The greater the reward, the greater the risk of penetration into a system: this is the concept of attractiveness of an organization as a target.

ICT Security managers should take into consideration the following outlooks and measures

Consider security as a permanent process that includes resources, costs, and processes optimization within a risk management framework

Define specific security policies to support business activities (security reference model), crisis management policy (back-up solutions) and business continuity

Configure and manage hardware and software securely

Acknowledge their own legal responsibility in the event of major security incidents or crises

Develop information assurance and legal conformity

Manage human resources - perform thorough background checks and allocate responsibilities clearly and sensibly

Figure 11.6 Some basic principle in security management.

Security is a matter for everyone

Each person using an information and communication device, tool, or service, for professional or private issues, needs information security. It is true for governmental institutions as for big or small organisations and individuals. The security answer should satisfy particular protection and defence level requirements regarding the actor's need.

Security approaches are often limited to the installation of risk reduction measures designed to protect the information technology resources of large organizations. However, the security approach must also necessarily meet the security needs of small- and medium-sized organizations, as well as those of end users (individuals). Individuals have a particular need to protect their personal or sensitive data, their privacy, and their basic human rights. As the Internet is global and has international coverage, all countries over the world need to develop and implement national cybersecurity policies.

For developing countries, attempts to reduce the digital divide through investment in infrastructure only, without taking into account the need for security and control of IT risks (unsolicited incident, malevolent acts, etc.), would result in the creation of a security divide as prejudicial as the digital divide. The use of a technological and legal approach would minimize the digital divide and more quickly create a reliable infrastructure that meets global cyber security needs.

It has become imperative that developing countries not only introduce measures to fight against cybercrime, but also control the security of their infrastructures and information technology services. Information security constitutes a driving force for the economic development of regions and must be developed and implemented simultaneously with the implementation of ICT infrastructure. The benefits to be derived from the deployment of information technology services are dependent upon the accompanying development of both the ICT infrastructure and an appropriate legal and regulatory framework. With sufficient security measures and effective laws, a digital economy can be developed. ICT security in a broad sense, including the legal framework, is critical for attracting players with the resources and drive to develop a favourable business environment. This is the main factor that guarantees that investment in infrastructure would be profitable. Of course, cybersecurity tools and the accompanying legal framework constitute an additional challenge for developing countries that want to participate in the global economy. An inclusive global information society would avoid pitfalls such as the emergence of digital paradises[2] or the exclusion of users from effective digital security.

Questions of responsibility and accountability

It is the responsibility of everyone to promote a safe and reliable cyberspace environment. However, to make this a reality, a minimum level of security for information and communication technologies must be provided at an affordable cost. Security must not become an exclusion factor for anyone who would like to conduct private or business activities over the Internet.

Technologies must have progressively fewer vulnerabilities and improved quality and security. The market must increase product liability, take into consideration the mobile world, and enforce identity management, authentication, and privacy. Only the parallel development of security control and privacy protection will generate confidence in information and communication technologies and in e-activities or e-transactions. Security needs must be taken into account right from the start when building infrastructure and considering accessibility.

Presently, most ICT end users do not understand the importance of security and privacy issues and possess neither the skills nor the tools to correctly protect their assets. They must rely on products and mechanisms they can neither understand nor master.

In the context of information security, some basic recommendations include:

- educating the end-user.
- increasing public awareness to improve users' behaviour in respect of security.
- providing the end user with the tools and the means to be responsible.
- designing an end user-centric security model within a given technical and legal framework whereby each user can choose, given his or her specific circumstances, the most appropriate approach to security.

Developing security models and solutions in isolation is not enough to protect information resources. If technical security measures have to be developed and implemented, concomitant legal measures must exist to prevent and deter criminal behaviour that uses pervasive networks as a target of crime

[2] A digital paradise is a country where no laws exist that criminalise computer related crime (including cybercrime and electronic crime).

(new technology – new crimes) or that uses pervasive networks as a means to commit crimes (old crimes with new technology).

Dependency upon ICT infrastructures is a reality, trust is a feeling, and security is a compromise. In this context, taking into consideration the responsibility of all actors involved in security (producers, consumers, private and public entities) and the various means of controlling security, a compromise needs to be made between cost, security service level, usability, and security efficiency. It is illusory to believe that these factors could all be satisfied at once, but at the same time, the end user's perspective and the reasons for requiring security should not be forgotten. The legal dimension of ICT security should be considered as a global business enabler that will minimize criminal opportunities.

It is mistaken to think that technological or legal solutions will compensate for design or management errors that occur at a strategic, tactical, or operational level.

The legal and technological worlds must be in harmony. Technology is not neutral, nor is the law. Their development should follow economic development and even become a driving force for the economy.

11.4 A systemic approach to cybersecurity[3]

The requirements

In this context, the word *global* should be understood as a systemic security framework that includes the political, social, economic, and technical dimensions of cybersecurity, at both national and international levels. The systemic approach involves all members of the information society: all types of end users (including children and older people), technologies, service and content providers and professionals, policy makers, organization owners, shareholders, managers, and justice and police professionals (such as judges, prosecutors, and law enforcement officers) (Figure 11.7). In a cybersecurity context, *global* also implies the necessity to think about security in terms of collaboration, cooperation, and sharing know-how.

[3] I had the opportunity to present and share my ideas related to a global and systemic approach of cybersecurity issues in several ITU's WSIS events from 2003 until today. Most of them have been already been integrated in several ITU's documents, such as the "Cybersecurity Guide for Developing Countries," that I have written (first edition 2006), and the HLEG report and GCA strategic report, to which I contributed. Within the ITU's Global Cybersecurity Agenda, I was co-leader of the working areas Organisational Structures and Capacity Building and an active contributor to the International Cooperation's working area.

From public awareness to policy makers, a global and timely cybersecurity approach should be available to answer all types of security issues and challenges. Each user of ICT has a role to play in the ICT security chain. At the same time, security is strongly linked to local culture, ethics, politics, and laws – thus to specific national environments – which means that in an interconnected global information society, cybersecurity should meet the challenge of being both locally relevant and efficient for a particular national context and interoperable and compatible at the international level.

Because of the global nature of cyberthreats and of the interconnected ICT infrastructures, a universal approach to cybersecurity is needed.

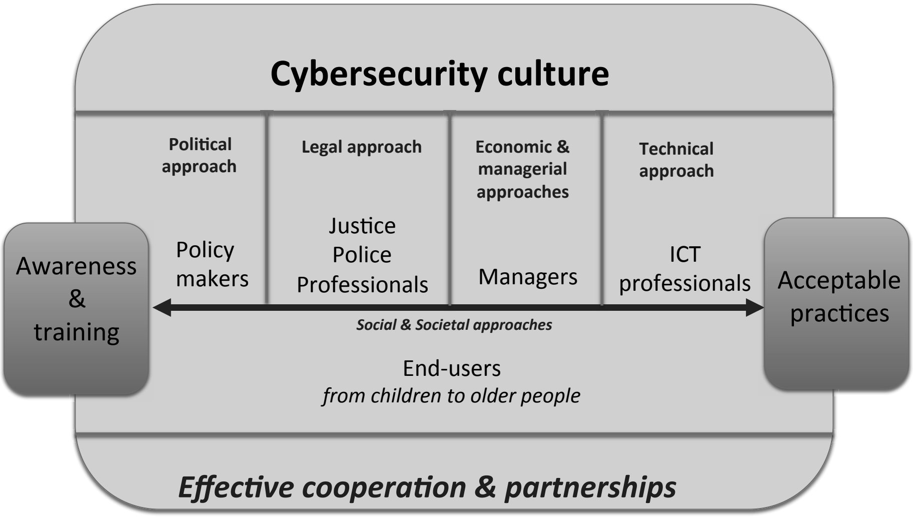


Figure 11.7 A systemic and global cybersecurity approach.

A universal approach of information security is useful in order to:

- have a common understanding of what cybersecurity means to all participants;
- contribute to building a global response designed to create a safe and interrelated information society;
- facilitate the definition and deployment of national cybersecurity strategies and structures for international cooperation;
- create local know-how based on well-recognized standards and good practices and address specific local needs by integrating local cultural values into national standards derived from these international standards and good practices;

- avoid the duplication of works and efforts;
- optimize the cooperation between all participants, providers, and public and private entities.

Coherent national and international approaches that address the need for effective cooperation could contribute towards achieving these goals.

The political dimension

Because cybersecurity and cybercrime issues are governmental issues and national security issues, the representatives of governments should understand:

- the links between ICT, social and economic development, and issues of criminality and cybersecurity in a connected world with interrelated infrastructures;
- ICT related threats and risks for states, organizations, and citizens, including privacy and economic and safety issues;
- the needs for protection at national, regional, and international levels;
- how ICT and the Internet have influenced the economic and military battlefields and the political and diplomatic landscapes;
- the roles of ICT in warfare, military activities, and state sovereignty;
- how ICT contributes to the modernization of states;
- what is at stake in the development of e-government services;
- the role of all relevant stakeholders and the relationships between private and public sectors;
- how to define general measures to be taken to obtain a satisfactory level of ICT security and protection of goods, values, and people;
- how to create appropriate national organisational structures;
- how to develop strategic improvements in ICT security;
- how to build and disseminate a cybersecurity culture.

The state holds a considerable responsibility for making digital security a reality. This is particularly true in the definition of an appropriate legal framework – one that is unified and practical. The state should not merely promote and encourage research and development in security; it should also promote security education and demand compliance with minimal security standards, while at the same time strengthening law enforcement of cybercrime. This raises the issue of funding and public-private partnership for national and international action plans.

At a strategic level, it is necessary to:

- ensure prevention, reporting, and information sharing and alert management related to cyberthreats;
- raise awareness of good practices in ICT risk management and cybersecurity;
- educate end users and increase public awareness to enhance users' behaviour regarding security;
- harmonize legal systems;
- provide assistance with regard to the promotion of law enforcement and security, both at national and international levels;
- propose and carry out cooperative ventures (formal/informal, multilateral/bilateral, active/passive, national/international).

However, 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 information technologies culture.

The state should encourage the different participants to develop the know-how and means to be able to manage the technological, operational, and information risks 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 in the economic world and the various 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 in the protection from, prosecution of, and recovery from cybercrime. The state must set up surveillance, detection, and information-handling centres for ICT and criminal risks.

It is up to each state to:

- define a development policy for the information society reflecting its own particular values;
- provide the resources necessary to make it a reality, including the means for cyber protection and defence.

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

The legal dimension

When considering the legal dimension and specific needs of justice and police professionals, the global understanding of legal issues related to ICT technologies and misuses should be understood as encompassing:

- legal requirements to fight against cybercrime and to protect people and society assets;
- the interpretation of the *Cybercrime Convention of the Council of Europe*, a document that can serve as an international reference model to define a legal framework and the appropriate cyberlaws enforceable at the national level and compatible at the international level, and that can also serve to develop measures to fight cybercrime and collaborate at an international level;
- computer related crime investigation and cyber forensic needs, challenges, and constraints;
- cybersecurity and digital privacy needs.

Policymakers need to create new legislation to complement existing laws, extending jurisdiction into cyberspace on the principle that what is illegal offline is also illegal online. 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.

The organizational dimension

Senior management of organisations of any size, including small- and medium-sized businesses, should understand the basic principles of ICT security management, in particular:

- the assessments of vulnerabilities, threats, and risks;
- the definition of security strategies and management practices.

They should also be able to address many of the following general issues:

- how to identify valuable assets and related risks;
- how to define and implement an ICT security policy;
- how to govern, manage, organize, control, evaluate, and optimize security policies and measures in complex and dynamic environments.

The goal of this is:

- to produce effective security processes and master ICT related risks and security costs; and
- to collaborate with legal, law enforcement, and technical professionals when necessary.

The technological and procedural dimension

In terms of the technological dimensions of cybersecurity, ICT professionals should:

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

The goal of that is 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 the availability, integrity, and confidentiality of ICT infrastructures and develop confidence in e-services.

Security technologies should be:

- cost effective;
- user-friendly;
- transparent;
- auditable;
- manageable even when provided by a third party.

In fact any security solution implemented in an ICT product in a default mode should be user-friendly, intuitive, transparent, and verifiable.

The human dimension

Every individual user should be able to understand:

- threats to the end user (viruses, spam, identity theft, fraud, swindles, privacy offences, etc.) and their impacts;
- how to adopt a security behaviour for a safe use of ICT resources;
- how to use security tools and follow security procedures.

Each individual (or organization) should be responsible for its attitude towards ICTs, and should adopt an ethical code of conduct. The Internet should be made into a common space open to all, without taking excessive security risks. Collectively, all players in cyberspace need to develop, consent to, and respect a uniform code of conduct and security ethics. People should be able to develop their own approaches to, and informed assessment of, how they should behave in respect of cybersecurity and the use of ICT.

The social dimension

At the present time, most ICT end users (individuals or organisations) simply do not understand cybersecurity issues and do not have the skills or the tools to protect their assets correctly. They do not have the objective means to build confidence in ICT infrastructures and services. They must rely on products and mechanisms they do not understand or master, and on solutions that have frequently been imposed on them for commercial reasons. Hence, security is based on obscurity.

So in order to empower human resources in a global perspective, a general, modular and flexible educational framework in cybersecurity should exist that will address the needs for increased public awareness and provide a deeper education for key professionals. This applies to developed countries as much as to less developed ones. Education is the key factor in becoming an actor in the information society, and it is the cornerstone of a knowledge-based society. Thanks to education, the digital literacy and the cybersecurity divide can be reduced. Therefore, to enhance confidence and security in the use of ICT and cybersecurity, education should not be considered optional.

Moreover, theoretically, it should be possible to give an end user the tools and means required to understand risks and responsibilities and to design an end user-centric security model within a given technical and legal framework whereby users can decide what is appropriate based on their own resources and needs.

Capacity building

Specific actions should be undertaken to foster capacity building in several areas of cybersecurity. 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 the strengthening of managerial systems. Capacity building in cybersecurity includes, in general, the following points:

- 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;
- organisational development, the creation 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.

Cybersecurity culture and education

The cybersecurity culture deals with key economic, legal, and social issues related to information security in order to contribute towards helping countries get prepared to face issues and challenges linked to the deployment, uses, and misuses of information and communication technologies. Cybersecurity has a global dimension and deals with a large range of issues, such as:

- ICT uses or misuses;
- technical measures;
- economic, legal, and political factors.

It is important to develop a general cybersecurity culture that raises the level of understanding of each member of the cybersecurity chain. Educational efforts and investments must educate and train all the members of the information society: from decision makers to citizens, including children and older people.

Specific actions should be taken at a national level to raise or build the cybersecurity capacities of various members in order to handle national and international cybersecurity issues. Both raising awareness and instituting specific education programs are difficult to achieve and costly. As capacity building activities take place at national level, appropriate resources should be made available. That requires financial, technical, organizational, and human resources. In some specific contexts, countries should benefit from international cooperation.

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 and effective educational programmes should be available for each kind of stakeholder, including policy makers, justice and police professionals, managers, information technology professionals, and end users.

At the beginning of these efforts, cybersecurity training courses should be integrated into different levels of the educational system, from schools to universities, and be included in education in the legal, scientific, and social science fields. Developing the interdisciplinary approach to 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.

The ICT level of penetration or internet uses vary from country to country, and even if cybersecurity problems are similar, the way to deal with those problems depends, 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 similar cybersecurity needs. So 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 and designing cybersecurity culture, one of the main challenges is to correctly identify the global and international issues and the local specific needs for a cybersecurity culture. International standards can only contribute to identifying the main global and generic issues related to a cybersecurity culture because cultures rely upon local and temporal factors. A unique and exclusive cybersecurity culture could be inappropriate in a specific information society environment. It could fail to respond adequately to the multitude of end user backgrounds, points of view, and needs.

Promoting a culture of cybersecurity that is relevant to the entire population must rely upon both an appropriate political vision and will and on efficient private and public partnerships. There are no real theories or methodologies related to how to design, communicate, validate, or 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, if the public and private sectors do not support such initiatives together as soon as possible, there will be, in the long-term, a negative effect on economic development and the ability to ensure the security of goods and people.

After all, the first two points of the OECD's 2002 guidelines for the security of information systems and networks – "towards a culture of security" are awareness and responsibility. There is a national responsibility to offer citizens the information on cybersecurity that they need to be effective and responsible cybercitizens. Sufficient awareness and education will help prevent incompetent or incorrect behaviours and develop trust and confidence in ICT infrastructures, services, security mechanisms, and controls. Education develops a layer of defence within a multi-level security approach that contributes to an effective defence. Education constitutes a genuine challenge that governments have to face.

11.5 Summary

ICTs have established a new network-oriented computer model. However, to facilitate the value added services that will make public or private organizations and individuals even more effective, it needs to be safe. In light of the new dimensions that ICT technologies add to economies and societies, cybersecurity is of fundamental importance and must be approached strategically. All Internet stakeholders should be aware not only of the importance of the security issues involved but also aware of the basic measures that, if effectively implemented, can strengthen user confidence in information and communication technologies. To prevent technological and informational risks, an adequate level of security is expected for ICT infrastructures and services. Therefore, it has become necessary to correctly identify security needs to make decisions regarding the scope and nature of security measures to be implemented. Global security implies adopting a multidisciplinary and systemic approach to cybersecurity.

The information economy, among other elements, heavily depends on cybersecurity. Without the latter, the former cannot sustain its development. At the same time, cybersecurity depends on the development of technology, on organizational structures, on legal frameworks, and on international cooperation. Without effective cybersecurity the overall performance of the information economy in a region may not render the desired results. Developing nations, and less developed countries, may face significant challenges in meeting the requirements of the global marketplace without cybersecurity.

The lack of know-how in all the dimensions of cybersecurity (technical, legal, organisational, and human) may constitute a serious infrastructure deficiency that is widening the digital divide. States and organizations must take steps to foster a culture of security regarding ICT usage and to develop a multidisciplinary approach toward security. They need to control the risk that ICTs will be used for criminal purposes. They must provide education, information, and training not only in security and deterrents, but also in data processing and communication technologies. Heightening awareness of security issues must not be limited to promoting a culture of security; instead, it should rely on a genuine ICT culture.

Using computers, networks, and information resources via the Internet necessitates mastering technological and informational risks in order to allow an efficient use of these technologies. It is not enough to promote development of connecting points to the Internet for accessibility; the information infrastructure must be reliable. This means that ad hoc performances, services continuity, quality of service, and quality of data must all be guaranteed. At the same time, national legal frameworks should exist and conform to international regulations to prevent misuses, to fight against cybercriminality, and to protect civil liberties and fundamental human rights.

Promoting a culture of cybersecurity contributes to building a safe and inclusive information society. Education is a long-term strategy that is necessary and efficient for a sustainable information society.

All participants in the Internet should be aware of the basic steps required to strengthen the level of security. Civic education for a responsible information society and information campaigns that cover the challenges, risks, and preventive and deterrent security measures must set and achieve this goal. Information campaigns should emphasize individual responsibility and deterrent measures, as well as the legal measures in place to enforce security obligations. More generally, it is necessary to provide education and training in ICTs. The awareness of security issues should not be limited to the promotion of a certain security culture. The security culture must be embedded within an ICT culture.

ICT security is interdisciplinary by nature. It lies at the crossroads of technological, legal, sociological, economic, and political fields. It must reflect the vision, culture, and civilization of each nation and also meet the specific security needs of the local context in which it is introduced. To put together the pieces of a global cybersecurity puzzle, answers should be provided by informed participants representing the political, legal, organisational, technical, and social dimensions of cybersecurity.

Security solutions do exist, but they are never absolute, and they generally represent no more than a response to a particular problem in a specific context.

In many cases they are purely technological in nature, and, like all technology, they are fallible and can be circumvented. Typically they merely displace the security problem and shift responsibility to another part of the system. 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 evolving technologies and malevolent skills, 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 is not sufficient; it must be integrated within a broad managerial approach.

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

11.6 Exercises

1. Why should cybersecurity be addressed from a global perspective and following a systematic approach?
2. To what extent can cybersecurity be seen as a political, economic, and social problem?
3. What are the principal factors in the evolution of information security?
4. Why is it not possible to address information security from a purely technological perspective?
5. Why is it important not to allow the digital divide to be replaced by a cybersecurity divide?
6. To what extent does cybersecurity affect everybody?
7. Explain the different ways in which the concept of responsibility can be applied to cybersecurity.

8. Considering the different dimensions of cybersecurity, identify the human abilities that need to be developed within a country for that country to draw on the necessary skills and experience.
9. What are the differences between cybersecurity awareness and cybersecurity education? Explain how these concepts are complementary.
10. Identify the activities that develop a cybersecurity culture for the citizens, both young and old, of a country and for the employees of an organisation.

Chapter 12

Cybersecurity Governance and Security Measures

12.1 Understanding the context

A strategic vision

At the start of the 21st Century, most large organizations – and many smaller ones – have accepted the importance of facing up to the challenges of cybersecurity. They no longer view security strategy as merely an unstructured selection of security tools; instead, it is widely viewed as an ongoing management process.

Approaching security through a dynamic management process that continuously adapts and improves solutions helps an organization deal with the dynamic nature of security risks.

The goal of ICT security governance is to ensure that organizations use the most suitable security measures at each given place and time regarding the risks faced. Figure 12.1 presents some of the most critical questions that should be taken into consideration for the development of a security approach. These questions are simple to express and amount to little more than common sense. Answering them is more complex and often represents a difficult objective for security managers to achieve, especially when taking into account additional organization-specific questions, such as:

- Who is actually in control of security?

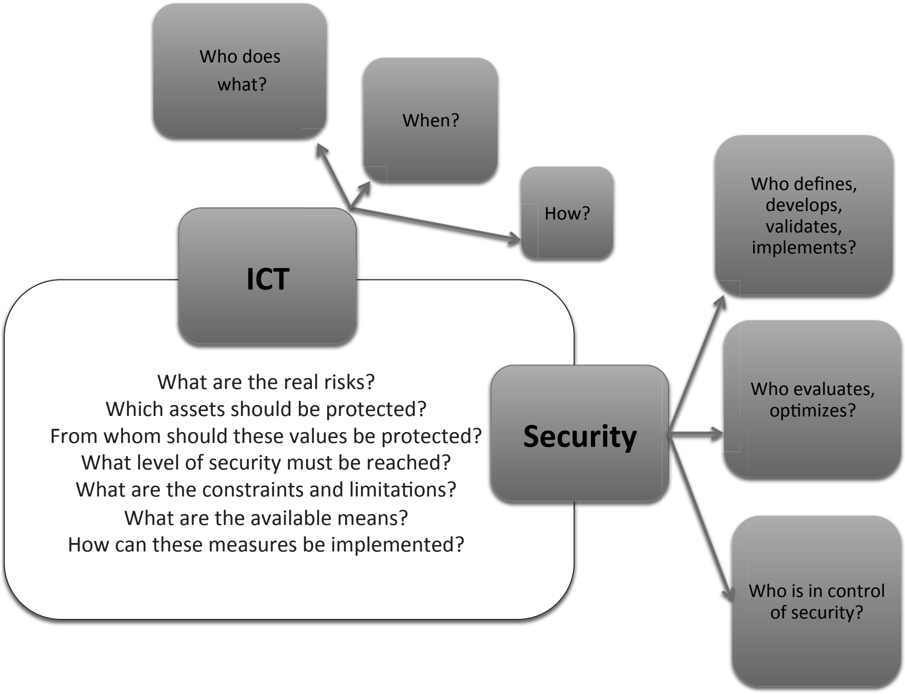

Who does what?
When?
How?
ICT
Who defines, develops, validates, implements?
Who evaluates, optimizes?
Security
Who is in control of security?
What are the real risks?
Which assets should be protected?
From whom should these values be protected?
What level of security must be reached?
What are the constraints and limitations?
What are the available means?
How can these measures be implemented?

Figure 12.1 Fundamental ICT security related questions to be answered.

- Who are the key players: who develops, defines, validates, and implements the necessary procedures, and then monitors their performance?
- Regarding the use of ICT, who does what, how, and when?

The security efficiency of e-services and applications does not just depend on security tools; it requires a coherent strategy, appropriate changes within the organization, and the implementation of additional and complementary sets of procedures. All of this requires an adequate control structure, the mission of which is to explain the importance of security and to manage, implement, validate, and control the various security measures. In addition, this control structure also determines the behaviour, privileges, and responsibilities of all users and specifies the appropriate security measures and directives that are related to critical success factors for the organization to reach its business targets. It must be consistent with both the overall business and information technology plans. To accomplish this it is necessary to develop a strategic vision of the enterprise's overall security needs and profile. A security policy must offer a graduated response to each specific security problem, in accordance with the risk analysis done in a given situation.

Following a number of basic principles that form the main conditions for success will usually ease the implementation effective security measures:

- strong direction and senior management involvement;
- identifying and avoiding dangerous situations;
- a simple, precise, understandable and feasible security policy;
- the publication, and availability to staff, of the security policy;
- centralised management and appropriate automation of security processes;
- definition of the required level of confidence of people, systems, procedures, and tools;
- trained and competent staff with high moral standards;
- definition of requirements for the control, respect, and validation of security clauses in employment and operational contracts;
- clear business ethics and respect for legal constraints;
- logging, monitoring and auditing measures;
- taking into consideration regulatory and legal compliance requirements.

The choice of security measures is a result of a trade-off between the cost of the risks and the cost of their reduction, and also between the need for productivity versus the need for protection.

The choice is derived from an analysis of the long-, middle-, and short-term security requirements and approaches (Figure 12.2).

The multidimensional aspect of security can only be fully understood from a global and centralised perspective. From general directives specified by the security policy (strategic axis), measures are determined (tactical axis), and tools identified (operational axis) that are then implemented locally in line with the nature and planned use of each technology (Figure 12.3).

This global and strategic understanding of information security is based on the following key elements:

- the definition of a security policy;
- the motivation and training of staff;
- the implementation of both proactive and reactive measures;
- the optimisation of the use of information and communications technologies as well as security solutions.

The use of security tools alone cannot solve an organization's security problems. They can never replace the consistent management of risk analysis and of the background to security issues. Security requirements need to be clearly identified and constantly re-evaluated in respect of the risks to be addressed and the evolution of these risks.

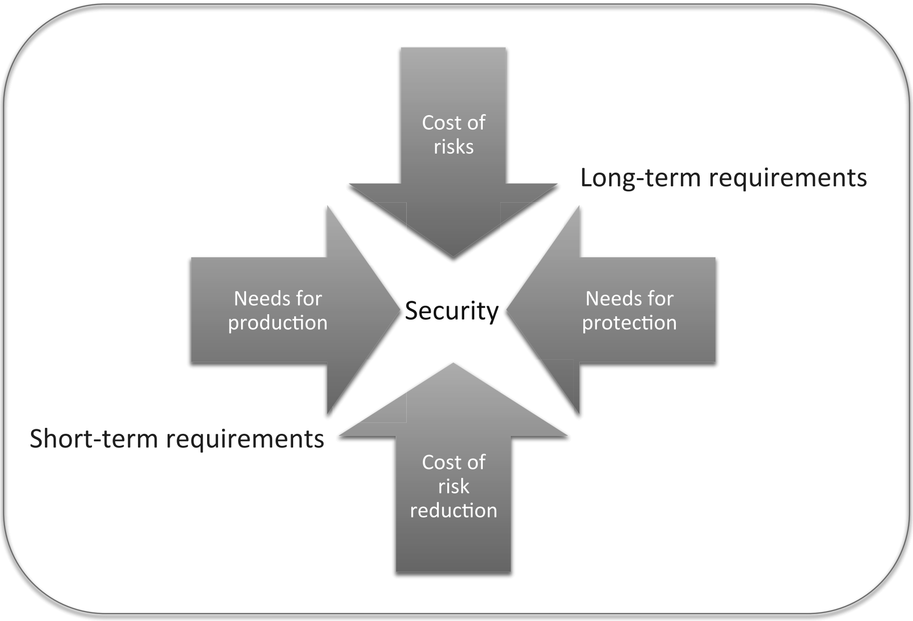
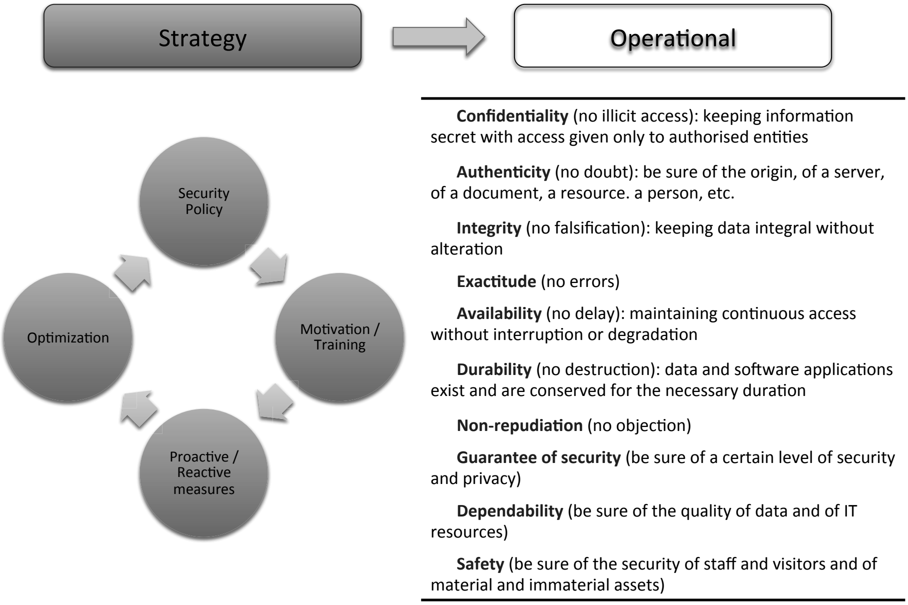


Figure 12.2 Security is the result of a compromise.



Confidentiality (no illicit access): keeping information secret with access given only to authorised entities

Authenticity (no doubt): be sure of the origin, of a server, of a document, a resource. a person, etc.

Integrity (no falsification): keeping data integral without alteration

Exactitude (no errors)

Availability (no delay): maintaining continuous access without interruption or degradation

Durability (no destruction): data and software applications exist and are conserved for the necessary duration

Non-repudiation (no objection)

Guarantee of security (be sure of a certain level of security and privacy)

Dependability (be sure of the quality of data and of IT resources)

Safety (be sure of the security of staff and visitors and of material and immaterial assets)

Figure 12.3 A strategic and operational approach to security.

The disorganised proliferation of security tools that are not properly integrated into a managed, continuous security process will only lead to interferences with usages, making the operation of an information system more onerous, increasing the costs or reducing the performance.

A rigorous monagement approach

Information security also requires the rigorous management of human resources, information systems, networks, buildings, and the environmental infrastructure. The control of information security is, above all, a management question, for which the tools, functions, and solutions make up a part of the operational administration of systems. Tools such as encryption or firewalls cannot ensure the security of an operating environment unless they are appropriately included in a specific risk management process and are accompanied by procedures that govern their configuration, administration, and use. Thus, managing security corresponds to the willingness to master the risks linked to the use of information technologies and the costs incurred in protecting information systems from threats. It also means deploying the necessary resources for handling incidents and crises and reacting to unexpected situations that threaten the performance of the information systems or the organisation as a whole. Managing information security and telecommunications is an activity with impacts in the fields of human relations, organisational management, management, and economics, and it requires a political desire on the part of senior management to manage risks and protect the assets of the organisation.

Thus, security relies on managerial, technical, and legal aspects that must be addressed in a complementary manner. Security is never definitively achieved: the constant evolution of needs, systems, threats, and risks means that all security measures are potentially only temporary. This leads to a problem of managing consistent quality in a complex, dynamic, and evolving environment. In this context, information security can only be understood as an ongoing management process designed to address in an optimal way (in terms of costs and the level of security provided) the organisation's requirements for supporting its activities and protecting its assets.

For many businesses, information technology is a key tool for daily activities and future development. In such cases, the unavailability or malfunctioning of systems is a major risk. This risk can nonetheless be reduced through the rigorous management of resources and their security.

Information security and quality requires the satisfaction of requirements regarding profitability and competitiveness, while improving the business's performance with a properly secured information system. The ultimate objectives of an organisation that is working towards securing its information assets, resources, and processes are to deliver services or products with guaranteed quality and security.

12.2 Managing the risks

A risk awareness approach

Cybersecurity risks are those associated with information processing, computer systems, and telecommunications related to the use of Internet environments. These are also sometimes referred to as computer risks, information risks, or ICT risks. *Risk* may be defined as a danger that can be anticipated. 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.

Two key notions arise in the evaluation of risk: threats, which are the potential causes of indesirable incidents, and weaknesses, vulnerabilities or failures. A risk is the product of the probability of an event, based on the vulnerabilities inherent in the environment and the threats that exist, and the consequences of an incident:

$$\text{Risk} = (\text{Vulnerability, Threat, Impact})$$

The terminology associated with risk management distinguishes between the analysis, assessment, understanding, handling, and management of risk, as explained in Figure 12.4.

ICT risks that are operational by nature need to be identified along with the strategic, social, and environmental risks facing the organization. A sound analysis of both risks and security needs makes it possible to define an ICT security strategy that can than be translated into a policy. Answering these main questions contributes towards mastering ICT risks:

- Who will be in charge of risk analysis and risk management?
- What is the best way to conduct the analysis?
- What tools and methods are available?
- How reliable are these tools and methods?
- How much emphasis will there be on results?
- What are the costs?
- Would it be better to outsource this function?
- What are the risks, their origin, and their impacts?
- Which risks is the organisation obliged to manage?

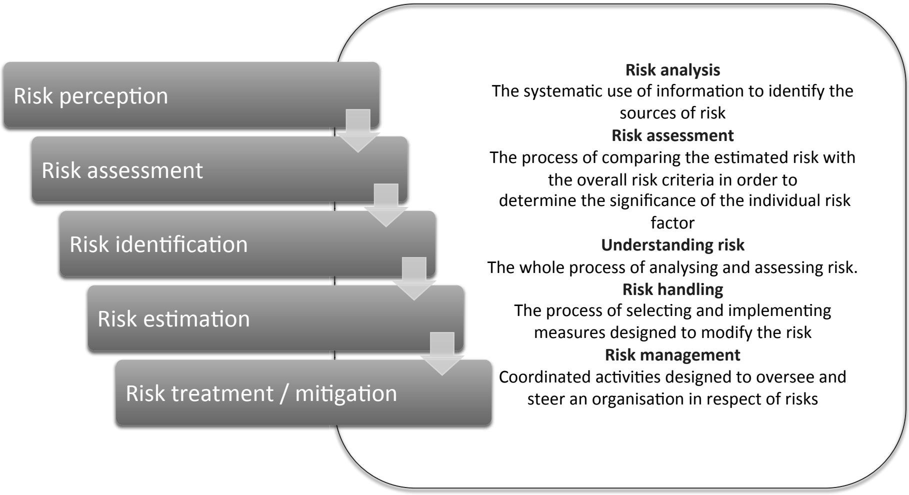

Risk perception
Risk assessment
Risk identification
Risk estimation
Risk treatment / mitigation
Risk analysis
The systematic use of information to identify the sources of risk
Risk assessment
The process of comparing the estimated risk with the overall risk criteria in order to determine the significance of the individual risk factor
Understanding risk
The whole process of analysing and assessing risk.
Risk handling
The process of selecting and implementing measures designed to modify the risk
Risk management
Coordinated activities designed to oversee and steer an organisation in respect of risks

Figure 12.4 Main risk-related terms.

In deciding on the desired level of protection and the security measures, 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 strategy, defining a security policy, and deciding on its tactical and operational implementation.

The main elements within an approach for managing information risk are the following (Figure 12.5):

- the identification of assets, based on security criteria;
- an understanding of the vulnerabilities that affect these assets;
- an understanding of the threats (identification of their origins, of the motivations and scope to be exploited, and of inhibiting, amplifying and catalysing factors);
- an understanding of the risk (often documented as a matrix of probabilities and impacts); and
- the definition of counter-measures (which take into account the three domains of activity, which are the processes, the technology, and the users).

A security strategy thus consists of designing a general plan for protection, prevention, and the organisation of defensive measures (a proactive approach); then plans must be developed to react to crises, for continuity management, and for the management of any resulting legal issues (a reactive approach). This is part of an approach based on business intelligence that allows the real control of operational, technological, and information risks.

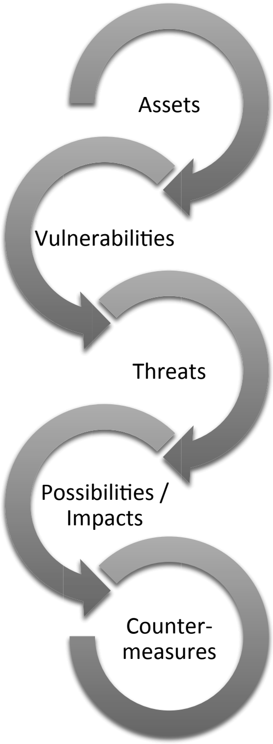


Figure 12.5 Trade-offs in controlling risk: a policy decision and a management process.

An economic challenge

The first objective of information security is not to make money, but to avoid losing it as a consequence of a security incident that caused either direct financial losses or indirect ones as a result of damage to the organisation's reputation or image. In this context, then, it might appear relatively straightforward to estimate what security actually costs: associated budgets, cost of security products, training, etc. However, assessing the profitability of security is more difficult. Taking a subjective approach, one might suppose that effective security measures intrinsically and passively lead to a measureable long-term profitability.

Nonetheless, it is difficult to compare the cost of security with the costs associated with losses due to accidents, errors, or malicious acts. The cost of security is related to the value of assets and to the organisation's specific needs with regard to the potential costs arising from insufficient security. Unfortunately there is no simple and unique answer to the following questions that arise when defining security objectives:

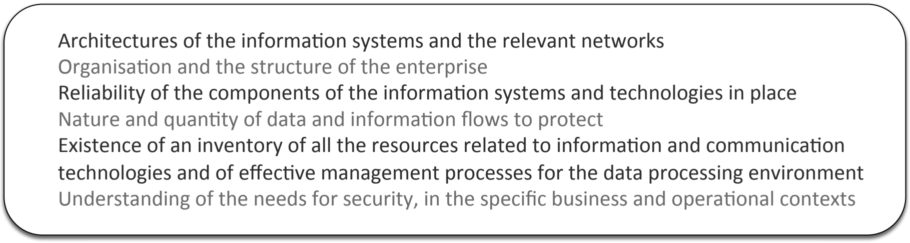
- How can the organization's risk exposure be evaluated, especially with regard to the sequential risks that are due to the interconnection of infrastructures between organizations?
- How can the indirect costs from a lack of security, such as those associated with damage to corporate image or espionage, be estimated?
- What concrete advantages can effective security provide for an organisation?
- What is the economic value of security?
- What is the return on investment of security?

In this context, it is essential that the economic value of security is considered in the broadest social sense rather than simply being reduced to the costs of installation and maintenance of security technologies.

Organisations and individuals must appropriately invest in information security, particularly to protect their critical resources. Given the evolution of cybercriminality, the only option is to be prepared to confront information risks that have criminal origins. It is only a matter of time until information systems become the targets or the means of attack. Properly securing the information environment can also give a competitive advantage, since criminals tend to attack the weakest entities first. In addition, adequate security allows organisations to respond better to security incidents and technical failures that have internal causes.

A consequence of the logic of the optimisation of the costs and effectiveness of security measures is that only the resources that strictly require structured security should be included in the security perimeter. Thus, it is necessary to classify resources according to their importance and need for security. This process also allows the prioritisation of security activities. Figure 12.6 presents some main variables related to the inherent costs of a security approach.

There are at least two activities that should be carried out in-house before the possible intervention of external security experts. These activities, which contribute to the reduction of the costs related to adopting a security approach, are linked to the correct identification of the following elements:



Architectures of the information systems and the relevant networks
Organisation and the structure of the enterprise
Reliability of the components of the information systems and technologies in place
Nature and quantity of data and information flows to protect
Existence of an inventory of all the resources related to information and communication technologies and of effective management processes for the data processing environment
Understanding of the needs for security, in the specific business and operational contexts

Figure 12.6 Principal factors that influence the cost of an ICT security approach.

- the data processing and telecommunications environments within the organisation, including hardware, software, data and programs, distribution, data and information flows (sources, recipients, telecommunications and technologies used, etc.);
- key users and managers of each information system (people, responsibilities, location, objectives, etc.);
- existing level of security; and
- level of security planned or required.

Insuring against risk is an activity motivated by financial protection and is not a preventive measure. It is a complementary action that should be undertaken to minimise financial losses caused by a disaster, not to avoid it. The insurance of electronic installations and data processing sites generally covers deterioration or destruction that occurs suddenly and without warning and is the consequence of an external event caused by:

- errors in manipulation, negligence;
- conscious prejudicial acts;
- equipment being knocked over or falling;
- atmospheric pollution, foreign bodies;
- effects of humidity and temperature;
- overloads;
- vibrations;
- fires, explosions;
- natural disasters (storms, flooding, etc.); and
- loss through theft.

However, not all risks are insurable. The value of the object of the insurance has to be known; here the complex problem of the quantification of the value of information is encountered and, with it, the calculation of the amount to be paid for a potential future claim. This constitutes a classic problem for the actuarial sciences. Premiums are calculated on a case-by-case basis, as a function of multiple factors, and they are often expensive and characterised by numerous restrictions. Unfortunately, insurance companies generally do not take into account whether effective security measures are employed by enterprises.

Generally, insurance companies insure for hardware damages and data loss. This is based on the value (when new) of all the equipment affected that is mentioned in the policy and on the costs related to the continuity of operations after a disaster. Since it is difficult to estimate the financial value of information and the related financial consequences of its loss, insurance policies only cover the cost of the recovery or recreation of the information, providing that its disappearance or alteration by an external action can be proven.

Since not all risks are insurable, alternatives must be found for non-covered risks. Three simple elements of response may be envisaged for minimising non-covered risks:

- avoiding the likelihood of an incident occurring by taking particular care over the relevant preventive measures, by systematically duplicating data and programs that are not covered by the policies (by implementing reliable backup procedures), and by reducing environmental risks, such as fire and flood;
- making financial provisions for losses;
- using best practices for the operation and maintenance of the infrastructure to prevent system breakdowns.

A compliance question

A number of instances of national law and international conventions legally oblige organizations – hence, their managers and security administrators – to implement security measures. However, the obligation relates to efforts, not results. Therefore, senior managers should pay careful attention to the law applicable to information technologies and information systems in order to ensure that they are in full legal compliance.

A legal entity that is guilty of a security lapse that leads to an infraction may find itself bearing a criminal, civil, or administrative responsibility for the consequences. Of course, whether or not such responsibility is ultimately established will have no bearing on the criminal responsibility of the individuals who were guilty of the infraction.

Security strategies need to be designed, implemented, and operated in line with legal or regulatory requirements. Those responsible for compliance will need to demonstrate that sufficient measures to protect information systems and data have been implemented if they are to protect themselves against accusations of failing in their security management duties. The stakes related to the control of legal questions related to information security are becoming ever higher; they touch on areas such as: data retention, the responsibilities of service providers and hosts, the management of personnel data, the cybersurveillance of staff, IT contracts, and electronic signatures. Competence in legal issues in the IT field equals a strategic advantage for organisations.

In terms of legal compliance, the controls implemented demonstrate that the relevant laws, regulations, contractual obligations, security policies, and other standards have been respected. This is done through identifying the relevant texts that apply to the organisation, protecting the different types of documentation, and informing staff about the consequences of using IT resources.

A question of outsourcing

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. Moreover, a quality control process must accompany the choice of a contractor (Figure 12.7).

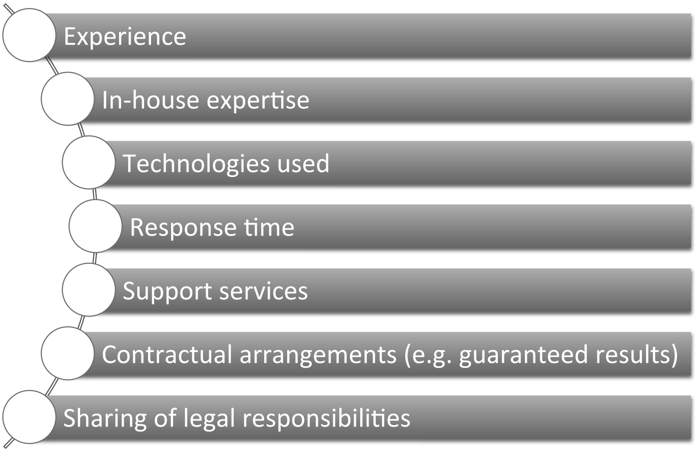

Experience
In-house expertise
Technologies used
Response time
Support services
Contractual arrangements (e.g. guaranteed results)
Sharing of legal responsibilities

Figure 12.7 Outsourcing: example of points to be taken into consideration for a quality control process.

A security outsourcing strategy may concern, for example:

- the definition of policy;
- the implementation of policy;

- remote maintenance of systems and networks; and
- back-up management.

The major advantage of an outsourcing solution rests essentially in the fact that the service is provided by security professionals who, based on their level of competence and experience, will be able to respond to security issues more effectively than in-house resources. But at the same time, this solution can create new risks for the business. Among the negative impacts are:

- the dependence of the business on the service provider;
- solutions that are not necessarily attuned to the internal processes or the values of the business, if these have not been sufficiently identified and communicated; and
- a weakening of responsibility for security problems within the business.

The most fashionable concept of the decade from 2010 is cloud computing.[1] This idea emphasises the evolution of the network and of service infrastructures. Now, more than ever, the network is key: computers, servers, processing, and data are separate but create a community of shared resources, shareable according to the needs of the users and available on demand. Users can theoretically access an infinite quantity of resources and almost unlimited processing power for a given period, without having to acquire and finance the necessary infrastructure. It is a question of paying for the actual, flexible use made of the facilities provided, according to various financial models (subscription, metered, etc.) proposed by the service providers. Thus, the use of IT resources is beginning to resemble the use of electricity. This concept has emerged from the technologies of shared processing (*grid computing*) used for scientific computing and research.

Certain providers offer services comparable to cloud computing that consist of using storage and data processing services on demand. Then the use of the IT infrastructure is viewed as a service provided by the third party. This can lead businesses to outsource IT applications that are seen as services for the relevant part of the business (the idea of the virtualisation of services). Cloud computing is based upon a large quantity of servers dedicated to storage and processing (server farms) as well as on a telecommunications infrastructure based on Internet technologies.

This vision of information technology does raise a number of technological, economic, legal, security, and environmental questions. It accentuates the

[1] This expression is derived from the schematics used in telecommunications, in which the overall concept of a network is represented by a cloud.

importance of the network, for without the network, it is impossible to access information and services that are located somewhere in the cloud. At the same time it increases the dependence on the providers of these services, on data centre operators, and on the network as a whole. At a geopolitical level, new risks and stakes are becoming noticeable.

This also creates new challenges for managing cybercriminality, as cloud computing naturally becomes a new playing field for cybercriminals. These groups and individuals see in the cloud opportunities for the automation of cybercrimes, optimised spreading of malware, or the hijacking of data and programmes belonging to cloud clients. In addition, cloud computing service providers can store the data and processing elements of multiple clients in the same infrastructure, even on the same servers. The separation and watertightness of these environments must be guaranteed.

The use of cloud computing services, like the use of outsourcing facilities, in the short term seems to be economically profitable, but at the same time, it raises substantial questions of security and responsibility that are as yet neither understood nor answered.

12.3 Defining a security policy

Objectives

The security policy translates the organization’s perceptions of the risks it faces and their impact into security measures for implementation. It facilitates both prevention and remedial action in response to security incidents. 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.

The security policy should specify, among other things, the resources, structures, procedures, and plans for defence and mitigation that will protect the organization from operational, technological, and information risks.

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 (Figure 12.8). Among the factors that contribute to the risk analysis are the organization’s size, image, areas of activity, system sensitivity, system environment and associated threats, and the degree to which the organization depends on its information system.

The quality of cybersecurity depends primarily on:

- identification and evaluation of the information assets;

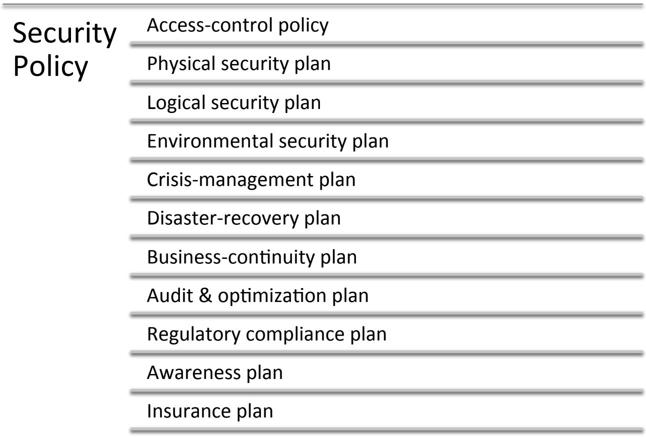


Figure 12.8 Some characteristics of an ICT security policy.

- operational deployment of appropriate security measures based on a well designed and up-to-date security policy;
- ethical uses of ICT;
- end-users' level of security awareness and behaviours; and
- effective management.

Fundamental principles

The quality of the management of security will determine the level of security provided. Cybersecurity policy should be defined at the level of top management. Although there are as many security strategies, policies, measures, procedures, and solutions as there are organizations with security needs, there are eight fundamental principles that, if the institution as a whole adopts them, facilitate the implementation and administration of information technology security (Figure 12.9). These are the following:

Definition principle: the need to agree, on enterprise level, on a common language to define security.

Coherency principle: an accumulation of security tools is not sufficient to achieve global and coherent security. The security of an information system is the result of the harmonious integration of tools, mechanisms, and procedures relating to the prevention, detection, protection, and correction of damage caused by error, malicious intent, or natural elements.

Management engagement principle: this principle results directly from the consideration of information as a strategic resource for the enterprise.

Hence, it is management's responsibility to provide the necessary means for the implementation and administration of a security plan.

Financial principle: the cost of security and the control measures must be proportional to the risks and known to the users.

Simplicity and universality principle: security measures must be simple, flexible, understandable, and applicable to everybody.

Dynamic principle: security must be dynamic in order to integrate the temporal dimension and the evolution of requirements.

Continuum principle: the enterprise must continue to function even after an incident. Emergency and recovery procedures are required for this purpose.

Evaluation, control, and adaptation principle: it is imperative to set up the measures, procedures, and tools that allow the continuous evaluation and dynamic adjusting of the security level of an information system. This allows both a better understanding of the variability of the security criteria and an improved validation of the adequacy of the present level of security given the evolving nature of security needs.

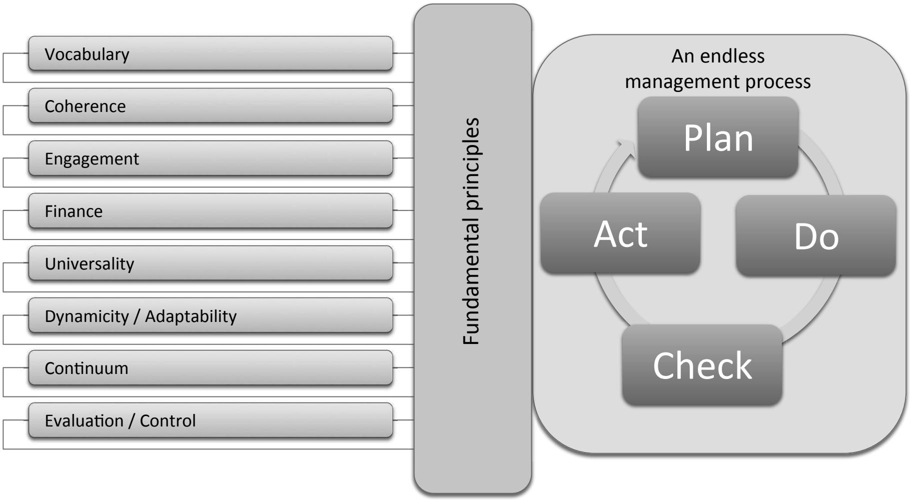


Figure 12.9 The most important principles related to information security policy management.

From risks management to security management

The security policy allows the application of the modelling work performed to understand the risks and their impacts to a set of concrete security measures and actions.

Its specification is one of the guarantors of the appropriate scoping and sizing of security measures and of effective management. It allows management to adopt a preventive and proactive attitude – not just a reactive one – toward risks and threats; it means that a security strategy can be linked to operational activities. Of course, the policy must be dynamic and subject to continuous reassessment in order to be adapted to the evolution of systems, environment, and risks.

The proper design of a security policy enables the effective management of data processing risks. However, even the best security manager, while able to anticipate and prevent certain incidents, is not a clairvoyant. Most security measures are based around managing data and systems, not predicting human integrity, and it is difficult to design even the most sophisticated measures without ultimately relying, to some extent, on the integrity of, for example, network administrators. The weakest link in most security structures is the human element – through criminal behavior, unwillingly committing errors, or as the victim of social engineering. Figure 12.10 presents the principal tasks of the security service.

Organisation management is responsible for:

- ratifying the security policy which contains the philosophy of the security program, the complete set of laws, and the 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 employees and managers,
- presenting the security budget to the board of directors; and
- approving strategic, tactical, operational, and security audit plans.

From a strategic security vision to operational security measures

The use of a methodological approach is recommended because a security policy involves a set of procedures and directives. The directives are drawn up according to a risk analysis. This minimises threats and their impacts by means of preventive and dissuasive measures and also by corrective measures that protect the business's critical resources.

Security management is made easier if it is performed within the framework of a methodological approach to management.

The creation of a security strategy and its translation into security policy make it possible to define the overall desired level of security. It is then pos-

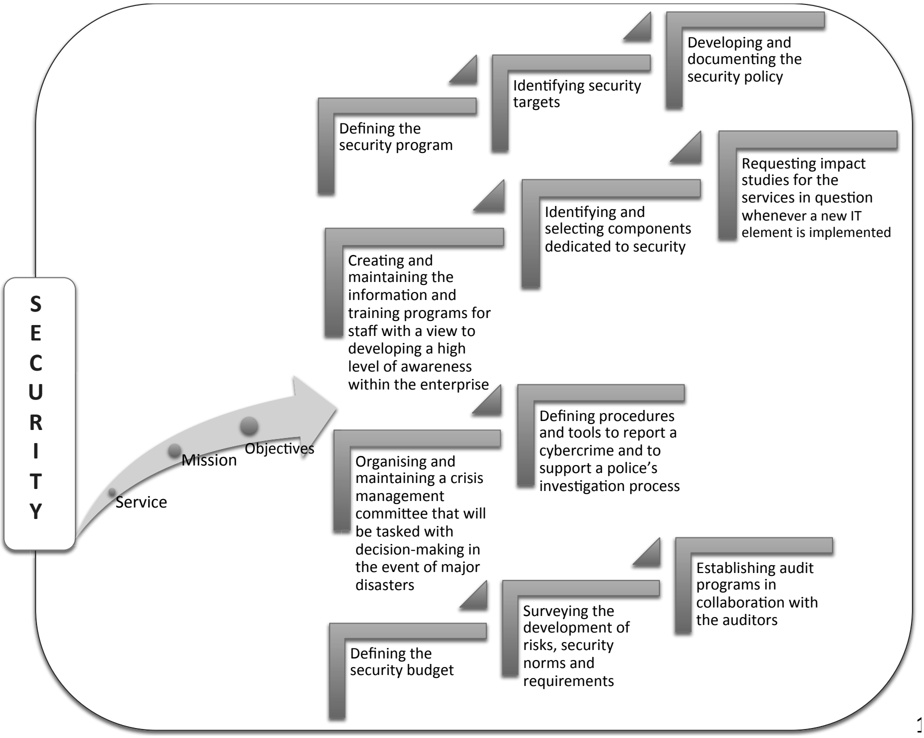

S
E
C
U
R
I
T
Y
Service
Mission
Objectives
Developing and documenting the security policy
Identifying security targets
Defining the security program
Requesting impact studies for the services in question whenever a new IT element is implemented
Identifying and selecting components dedicated to security
Creating and maintaining the information and training programs for staff with a view to developing a high level of awareness within the enterprise
Defining procedures and tools to report a cybercrime and to support a police's investigation process
Organising and maintaining a crisis management committee that will be tasked with decision-making in the event of major disasters
Establishing audit programs in collaboration with the auditors
Surveying the development of risks, security norms and requirements
Defining the security budget

Figure 12.10 Main security service tasks.

sible to translate these specifications into concrete actions and measures, by establishing the best adapted technological, organisational, and procedural tools.

A technological security survey can be seen as continuous auditing process of general security risks and market solutions. It is performed as part of the process of anticipating security requirements and solutions. Such a survey falls onto the strategic, tactical, and operational security axes. It allows management to remain vigilant and to identify potential threats before they materialise, to discover new software faults, and to recognise the signatures of acts of vandalism. This information contributes toward adapting the security policy and selecting and applying the best existing solutions.

The identification of security objectives in correlation with the sensitivity of resources leads to the definition of concrete measures to achieve these objectives. These are classified in several categories (Figure 12.11).

- *Structural measures* (such as masking resources, planned redundancy, and information fragmentation) contribute to protect the organization's assets.

- *Dissuasive measures* (such as legal and administrative procedures, awareness training, management of human resources, work conditions, and means of detection and tracing) avoid threats materialising, while preventive measures (such as logical and physical access controls and virus detection) ensure that attacks (or security incidents, malevolent acts, or errors) do not succeed in causing damage. A successful attack will cause a certain level of deterioration that could lead to financial losses or damage to the enterprise's public image.
- *Protective measures* (such as coherence checks, intrusion, fire, humidity and transmission error detection, and firewalls) protect against attacks and limit their effect.
- *Palliative or corrective measures* (such as backups, continuity plans, redundancy, repairs, and corrections) repair the damage caused and recovery methods (such as insurance and law suits) limit the losses following incidents.

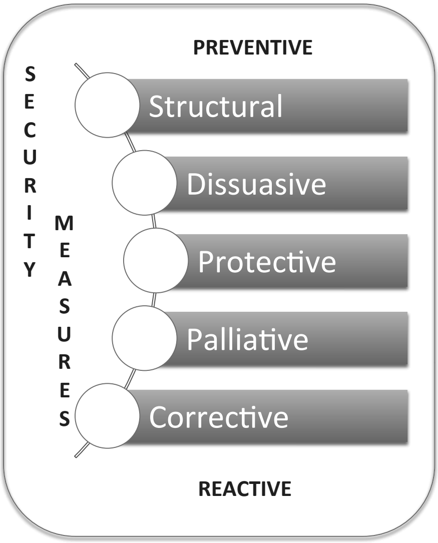


Figure 12.11 A typology of information security measures.

A preventive approach to security is, by definition, proactive. It is based on the identification of the assets to be protected and on the analysis of both risks and their constitutive elements (vulnerabilities, threats, impacts, likelihoods). Such an approach allows management to anticipate incidents, to control and minimise the likelihood of such incidents occurring, and to minimise the potential impact.

A reactive approach places the focus on the way incidents are handled once they occur. In general the emphasis is placed on the procedures designed to identify the problem so that it can be isolated and prevented from spreading further and so that losses are minimised, activities are continued, and the normal operating state is restored as quickly as possible.

A proactive approach also includes elements from a reactive approach, insofar as such an approach needs to be anticipated, planned, organised, and managed.

To the extent that zero risk does not exist, security measures belonging to these two complementary approaches need to be identified in a security policy.

Emphasising the technical dimension of an information systems security and neglecting the human dimension can create a serious problem in controlling the technology risks associated with criminal acts. Criminality is primarily a human issue, not a technical one. Therefore, a purely technical response is inadequate.

The typical approach toward cybercrime is one of reaction and prosecution. Therefore, action comes after the occurrence of an incident, which, by definition, has highlighted a weakness in the security measures. An organization needs:

- to prevent and deter cyberattacks by developing investigative/criminal mechanisms; and
- to identify the measures that are needed to respond to attacks and prosecute the attackers.

It must design and implement backup and continuity plans, incorporating the constraints related to the investigation and prosecution of cybercrime within the different work processes and objectives, within specific time scales.

12.4 Understanding ICT security from a technical point of view

Security as a part of system functionality

Information and communication security has as a primary motivation to ensure the usability of systems:

- The capability of a system to be used depends on the *availability* of hardware and software resources and services. It is a function of good dimensioning, sufficient redundancy of resources, and of backup, recovery, and operations procedures that are adapted to the requirements.

- The capability of a system to allow data access to authorised persons and processes only relates to the preservation of data *confidentiality* and *integrity*. These are ensured by access control procedures (identification, authentication, and authorisation with respect to certain permissions or access rights) and by encryption mechanisms.
- The capability of a system to allow data modification by authorised persons and processes only evokes the *integrity* criterion. It is produced by access controls, error controls, and coherency checking procedures.
- The capability of a system to prove that actions and transactions have really taken place provides 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 corresponds to a need for *continuity*, *reliability*, *user friendliness*, and *operational robustness*.

In this way, information security can be seen as a critical success factor for governmental, administrative, industrial, and business entities. It also contributes to reducing the chances that the credibility of an organisation could be put into question, by reducing the probability of threats actually being realised, by limiting the number of incidents (human error, natural accidents such as flooding or fire, criminal or malicious actions such as theft or vandalism), and, should an incident occur, by enabling a return to normal operation with acceptable costs and within an acceptable timeframe.

In most e-services, such as in e-government applications, security solutions do not generate revenues directly but help to avoid losing them, and optimise both administrative processes and communication between the involved actors. Quite simply, proactive and defensive strategies form a part of an economic intelligence approach. The following observations have helped leading organisations understand the evolution of information security needs and perceptions:

- the increased number of interconnected people, systems, and environments;
- digital information is vulnerable and volatile;
- growth in the number of hackers and improvement of their professional skills;
- real determination to protect information assets and a better understanding of security problems and consequences;
- information and communication technologies are complex;
- emergence of new forms of organisations, activities, business, etc.;

- need for a global control of security (integration and harmonisation of security tools, procedures, and measures leading to a globalisation of information system security);
- necessity to integrate security processes at the systems, networks, and enterprise management levels;
- reality of attacks against citizens, infrastructures, organisations, and governments entities (theft, swindle, fraud, deny of service, information warfare, cyberterrorism, cyberabuse, etc.);
- need for basic security fundamentals (audit, measures, intelligence, imputability, authentication) and for security resistance (proactive security protection, defensive and dissuasive measures).

Security criteria

Security solutions must satisfy basic security criteria, such as availability, integrity, and confidentiality (the AIC criteria). Other criteria that are often cited in this context are (Figure 12.12):

- authentication, which makes it possible to verify the authenticity of a claim (basically of the identity of an entity);
- non-repudiation; and
- imputability, which make it possible to verify that actions or events have taken place.

In designing solutions, care should be taken as well to protect the physical ICT environment. The spaces that house workstations, servers, IT areas, and services, such as air-conditioning and electrical supply panels, need to be physically protected against unauthorised access and accidents, such as fire and water damage. Physical security is the most fundamental and ubiquitous type of IT system control.

Availability

To ensure the availability of services, systems, and data, the components of the infrastructure systems must be appropriately sized and possess necessary redundancy. In addition, operational management of resources and services must be provided. Availability can be achieved by redundancy measures and enhanced by resilience and robustness of ICT infrastructure.

Availability is measured over the period of time during which the service provided is operational. The potential volume of work that can be handled

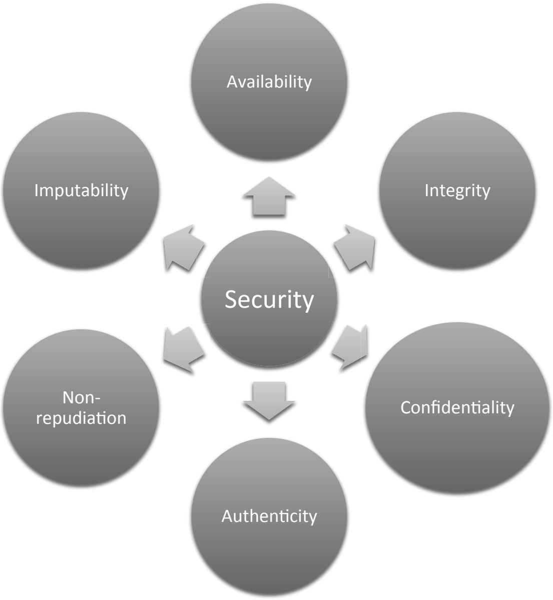


Figure 12.12 Main ICT security criteria.

during the period of availability of the service determines the capacity of the resource. The availability of a resource is closely linked to its accessibility.

Integrity

Preserving the integrity of data, processing, or services means protecting them against accidental and intentional modification, tampering, and destruction. This is needed to ensure that 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, for example:

- strictly enforced access control mechanisms;
- data encryption;
- protection against viruses, worms, and Trojan horses or any kind of malware; and
- intrusion detection systems.

Confidentiality

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 maintained through access control and encryption. In fact, 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.

Authentication

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 help achieve:

- 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 events or transactions: any action can be traced to an identified and authenticated entity; and
- proof of origin or destination: it can be proven that a message has been addressed to an identified and authenticated entity.

Being sure of an identity, a source, an entity, or an item of information, or being sure that an action has been correctly carried out enables the performance of tasks that contribute to a good quality of service.

Non-repudiation

In some circumstances, it is necessary to verify and prove 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 (concept of system auditability). This is particularly important for performing computer investigations to find system addresses used to send data or malware, for example. The investigators need to be able to record and retrieve the information that is to be used to conduct subsequent analysis for system auditing purposes (information logging).

Security measures must guarantee these properties, in accordance with the value and life cycle of the information. They must be implemented through specific tools and people, then managed and validated by administrative and audit procedures. Hence, security depends on a coherent set of measures.

12.5 A functional approach to generic security tools

Encryption

The encryption of data (cryptography) is the fundamental tool of security. Essentially the implementation of cryptography allows the operation of services ensuring the confidentiality of stored or transmitted data, methods of managing the integrity of data, and methods of authenticating entities, transactions, and operations, and of ensuring non-repudiation.

The implementation of methods of *symmetric encryption* that is based on the use of a single secret key to encrypt data on transmission and decrypt them on reception can prove to be efficient when considering the speed of the encryption and decryption activities (Figure 12.13 (a)). The major negative factor, however, is that every pair of correspondents must possess the same key, a situation that causes problems in the management and distribution of the keys. These keys (true secrets being used to protect secrets) need to be distributed and stored in a secure manner. In addition, this system is inappropriate in the Internet environment, functioning as it does essentially in a client/server mode, because if all the clients of a given server have the same key, nothing will really be confidential.

In a system using *asymmetric encryption*, two complementary keys are used to ensure the confidentiality of data. A unique pair of keys, consisting of a secret key (private) and a public key, is used for each correspondent. A sender who wishes to send data confidentially to a recipient will use the public key – which is known to everyone – of the recipient. When the encrypted data are received, the recipient will decrypt them using his own private key, which only he knows (Figure 12.13 (b)). Asymmetric encryption can be used to provide

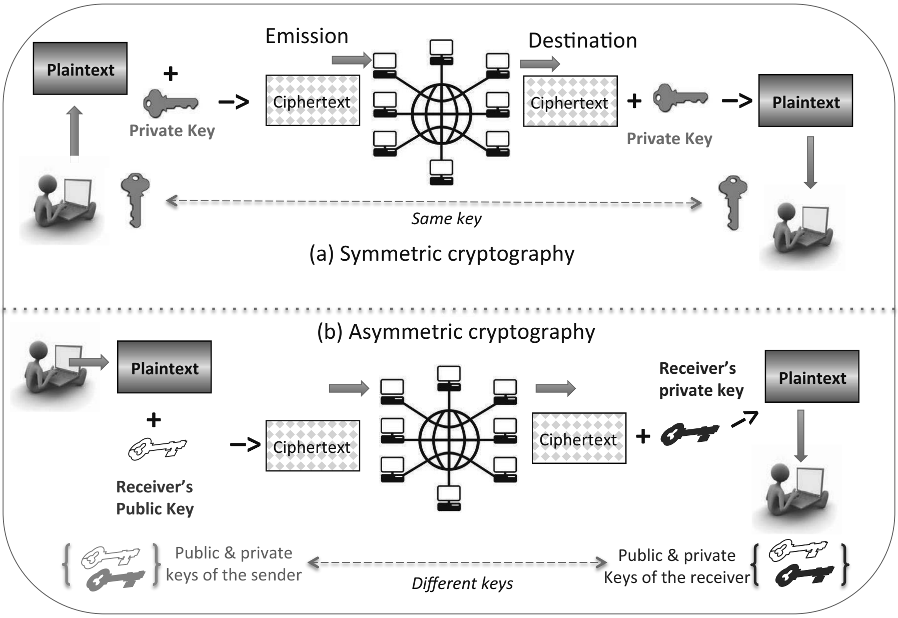


Figure 12.13 Assuring data transfer confidentiality by symmetric (a) and asymmetric cryptographic algorithms (b).

comfort over the integrity of data by using *hash (digest) functions*. In practice, for reasons of speed of the encryption of large volumes of transmitted data, a combination of symmetric and asymmetric encryption is often employed with the benefits of the advantages of both methods being enjoyed, at least in part.

In order to implement a system of asymmetric encryption, use needs to be made of a double key consisting of a private key (secret, known only to its owner) and a public key (non-secret, available to all who might need it). The main advantage of this approach is that there is no need to share a secret key. On the other hand, the management of the keys does require the use of an intermediary, an infrastructure for managing the keys (PKI, *Public Key Infrastructure*). The users need to register with this entity in order to obtain, in the form of a digital certificate, the necessary keys for secure communication. This approach allows, most notably, the operation of commercial and financial applications over the Internet[2] (Figure 12.14).

A *digital certificate* can be seen as the digital passport of either an organisation or an individual, and the means of enabling various activities and security services, such as a digital signature. Even though a digital certificate contrib-

[2] A PKI can also be described as a Certification Authority as it issues digital certificates, or a Recording Authority, based on whether client entities need to register to use its services.

utes to the security of transactions, it can be altered or falsified (for example, by a virus infecting the user's workstation). The management of a Certificate Revocation List (CRL), in which outdated certificates are recorded, increases the processing time for certificates and is only moderately effective. The field setting out the validity period of the certificate can be used to limit the lifespan of the certificate and allow, when the certificate is renewed, the modification of some of its parameters. This allows the performance of validity tests on certificates, based on its expiry date, and the management of changes within the organisation to which the certificate belongs.

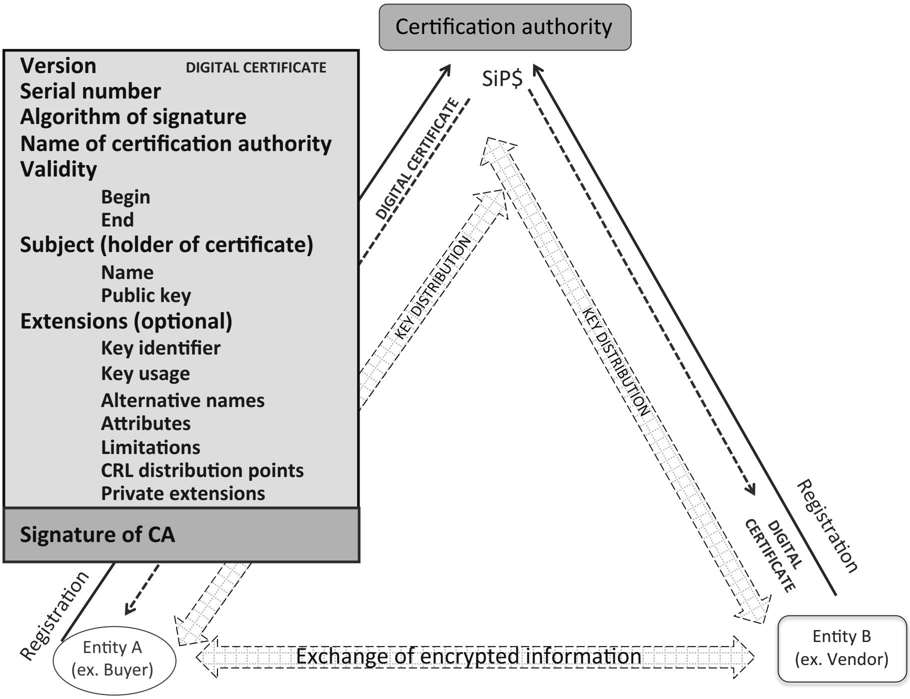


Figure 12.14 Public Key Infrastructure and digital certificates.

Thus, a PKI can contribute towards implementing the principles of asymmetric encryption and ensuring confidentiality, authentication, and integrity. Such an infrastructure addresses the need to possess encryption keys to carry out certain security tasks between users or entities who do not necessarily know each other. It also enables the recording of events to ensure traceability, imputability, and non-repudiation. On the other hand, the implementation of a PKI can generate a number of problems, such as:

- *Political problems:* the majority of PKI infrastructures and certification authorities belong to foreign entities. This raises various questions, such as:
  - that of *confidence* in those entities regarding the services provided (the creation, storage, and distribution of the public and private keys and of identification data, and the logging of events), in relation to the absence of guarantees over the non-abusive use of the data, and in relation to the neutrality of the service provider and the options for action on the event of disagreements with the certification authority;
  - that of performance and the availability of services;
- *Organisational problems:* such as the interoperability between different PKIs when correspondents do not use the same PKI. In addition, deploying, managing, maintaining, and ensuring the security of PKIs are complex and costly tasks. There can also be problems if the procedures for signing up to a PKI are not reliable, and without detailed examination and approval of the registration data provided by entities, the digital certificates issued will have no security value and could in fact contribute towards hiding the identities of wrongdoers by providing them with an additional layer of protection that slows down their identification.
- *Technological problems:* the security measures that are implemented to protect PKI can be avoided, encryption systems can be broken, and the hijacking of certificates, frauds, and deceptions are all still possible. Additionally, the use of a key management infrastructure passes the problem of the security of exchanges on to a new intermediary without actually solving it.

Generally speaking, the limits of asymmetric and symmetric encryption depend on the fact that their algorithms, based on mathematical logic, can be broken, and also on the keys that need to be managed as secrets (which can be discovered). One can add to this list the vulnerabilities of the information environments in which the encryption systems operate. An encryption algorithm is described as robust as long as cryptanalysis techniques have not yet demonstrated its fragility. Very often the idea of robustness is based on the resistance of the algorithms to various known methods of attack. But what is considered robust and relatively reliable today will not necessarily be so tomorrow!

However the various mechanisms and algorithms of encryption work, they are based on the use of keys. Generally, their level of robustness is linked to the ability to manage the encryption keys in a secure manner, to the length of the key[3], and to the security of the hardware and software platforms in which the encryption algorithms have been implemented and operated. The weakness factors of the keys are linked to their nature, their lifespan, and their use. The process of creation, distribution, retention, and destruction of keys has to be reliable and generate keys that are authentic, unbreakable, unguessable, and unpredictable. Keys that have become corrupted or fulfil no further use need to be blocked from further use and destroyed. Each of these activities presents security, management, and logistical problems. The major weakness of secret keys stems from the fact that they need to be secret and themselves secure (the idea of the recursiveness of security).

Confidence in encryption products can only be relative, in the sense that it is difficult to provide guarantees or means of verification that demonstrate that there are no backdoors hidden from users. In addition, secret keys can ultimately be duplicated or disclosed. And as discussed above, no proof can be given that algorithms that are considered to be reliable today will continue to be so in the near future.

The implementation of cryptography secures exchanges between users of e-services (as in the example of the use of a PKI) and also secures the communications infrastructures themselves by using communications protocols in which the encryption mechanisms are directly integrated. These are known as cryptographic protocols and can provide security services (authentication, integrity, and confidentiality). This is true of IPv6 (Internet Protocol) or TLS (*Transport Layer Security*[4]), for example. In fact, the majority of application protocols possess a secure version that frequently allows the authentication of users and the encryption of data being transferred.[5] An alternative to the implementation of new secure versions of the protocols consists of introducing a common security mechanism that provides generic security services to all applications. The TLS/SSL system, which is widely used nowadays for performing transactions on the Internet, fulfils this role (Figure 12.15).

Other security measures do need to be implemented to protect data transfers. It is fundamental that the addresses, processes, and systems involved in the management of names and addresses or in the routing of data are available, complete, reliable, and secure. The entities in charge of telecommunications infrastructures have the responsibility to protect and effectively manage their

[3] The length of an encryption key is a function of the type of algorithm used. Cryptographic keys required by asymmetric encryption are longer than those for symmetric encryption.

[4] TLS is the new denomination of the Secure Sockets Layer (SSLv3).

[5] As for examples HTTP (HyperText Transfer Protocol) ⇒ HTTPS or SMTP (Simple Mail Transfer Protocol) ⇒ S-SMTP.

operating environments and to provide access control mechanisms that correspond to the security criteria and the needs of users.

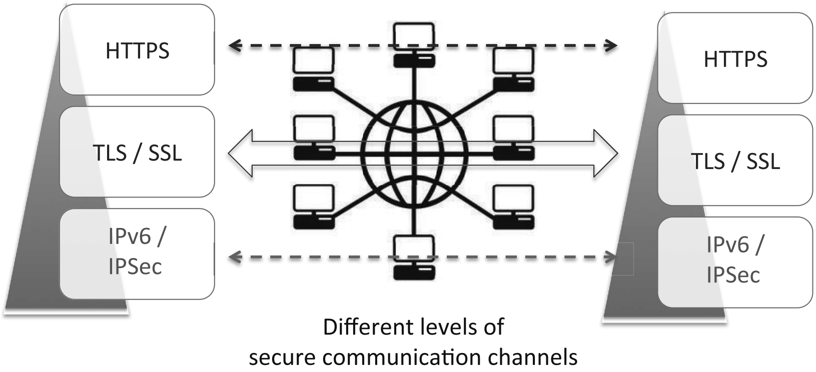


Figure 12.15 Main cryptographic protocols used over the Internet.

Access Control

Mechanisms of controlling logical access are based on the identification and authentication of users and on the permissions or access rights that have been allocated to them. Access to the requested resources is granted by the access control mechanism on the basis of the authenticated identity and of the user's profile (Figure 12.16). This supposes that the identification of the user (*Identity Management*), the proofs of identity (*Identity Proof Management)*, and the access rights are being managed correctly (*Authorization Management*).

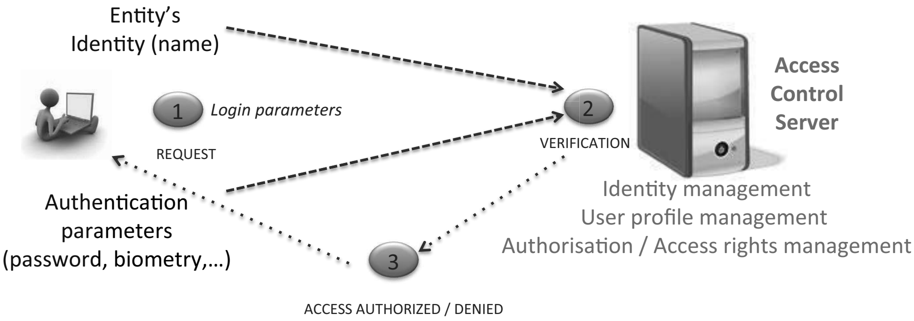


Figure 12.16 The access control mechanism.

The user profile contains all the information necessary for decisions about access authorisations. This profile, which needs to be defined very carefully, is the result of the definition of the policy relating to access management. When granting a user access to the requested service, the access control system performs a verification of the user's access rights that takes into account the consistency of the requested service, the equipment used, and the time and date of the request. The consistency review consists of comparing the profile of the service with the profiles of the user and of the system from which the request has been received. The authorisation will be granted when the user possesses the necessary rights to the service and when the hardware and software requirements are met and supported.

The objective of the authentication service is to verify that identities are genuine (the idea of the proof of identity). Generally this relies on one or several of the following factors:

- a secret that an entity *knows*, such as a password or PIN – *Personal Identification Number*;
- something that the entity *possesses*, such as a card or a token; or
- something that the entity *is*, such as a fingerprint, voiceprint, or retinal print.

Currently access control mechanisms are largely based on user IDs and passwords.

The verification of identity relies on a scenario in which the access requester provides his identity and a means of proof that he is supposed to be the only person to know or possess, such as a password, a confidential key, or a fingerprint. The authentication service then compares this information with data stored in an authentication server. This server clearly needs to be carefully protected and secured using ad hoc access control methods, secure system management techniques, and the encryption of the data it holds. An authentication server cannot be allowed to malfunction or be vulnerable because the overall security of the information and telecommunications infrastructure depends on how robust it is.

Security solutions themselves also need to be protected and made secure so that they can provide a certain level of security (the idea of the recursiveness of security). Thus, the in-depth security of information and telecoms systems is achieved by erecting a series of barriers (security tools and measures) that increase the level of difficulty for potential attackers to gain access to resources.

The application of biometrics[6] to access control allows the removal of the use of passwords by substituting them with a physical characteristic from which a piece of digital data can easily be extracted. When combined with "classical" mechanisms of authentication based on passwords, biometrics can reinforce the level of security – the idea of double controls. Biometric individualisation can be used to manage the identities of individuals in order to manage access to buildings or in the context of judicial proceedings. In order to use people's physical characteristics to identify them and validate their identification, it is necessary to record these biometric characteristics beforehand (the idea of sizing) (Figure 12.17). Of course, this acquisition of data must be reliable and consistent, and the storage of these data must be secure.

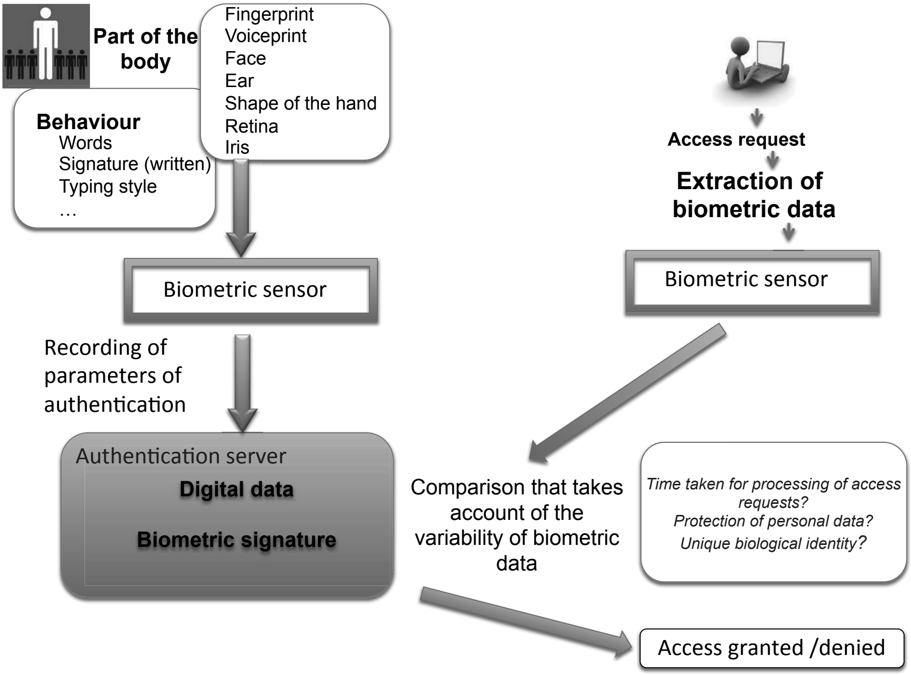


Figure 12.17 The principles of access control based on the use of biometric data.

[6] In fact, it is more a case of the application of "anthropometry," which refers to the "study of human body measurements especially on a comparative basis" (Merriam-Webster). This can lead, by the use of appropriate techniques, to the ability to identify individuals (and differentiate them from others); biometry itself is, strictly speaking, "the statistical analysis of biological observations and phenomena" (idem).

The process of authentication can take a long time because the comparison phase needs to take account of the inherent variations in the active characteristics of the data being tested. For example, as two voice samples from the same person will never be absolutely identical, the comparison needs to be based on statistical and probabilistic analysis of the biometric data. The aspect of imprecision thus drawn into authentication system means that it is impossible to obtain results of guaranteed exactitude (the system cannot guarantee at 100% that it is indeed person X who is trying to connect). The error rate in these systems remains high, a situation that does not allow the certainty of a high level of security. Alongside the lack of accuracy, the uncertainty over the ability to secure appropriately a database of biometric information, and the high costs of purchasing, implementing, and managing such systems mean that, at the moment, access control systems based on the use of biometric data remain suboptimal.

This type of solution has been applied for identifying citizens by using a biometric passport. This causes a number of problems for the security, management, and use of such biometric data, particularly in the context of the future evolution of such use by national and foreign governments and commercial entities.

If the process of the digitisation is to be undertaken, why should it be limited to two scans and not ten, such as the iris, the retina, the DNA, and then add behavioural data, health data, data on tastes, political opinions, sexual preference, religion…?

The widespread usage of biometrics raises numerous problems in the fields of ethics, ergonomics, economics, technologym and law. A small sample of these includes:

- the confidentiality and the protection of biometric data. If a piece of digitised data, such as a fingerprint, were somehow modified in a database, be it deliberately or by accident, the victim would need to try to prove their own identity using their own prints that now differ from those held digitally;
- the possibility of not being able to identify unique biometric *data* (as in the cases of identical twins);
- biometric data readers are often viewed, quite fairly, as being intrusive. These devices can be considered as a threat to privacy to the extent that public areas could contain numerous readers (video cameras, remote RFID readers) that gather data without the knowledge of the public, leading to the risk of the matching and merging of datasets relating to individuals; and
- cases of the usurping or abusive or fraudulent use of biometric data.

Firewalls and Intrusion Detection Systems

The widespread use of the Web and of online service has obliged many organisations to open their information systems towards the Internet. It has accordingly become fundamental for these organisations to protect properly their private IT and telecoms infrastructures and only leave accessible via the Internet those resources that are strictly necessary.

The fundamental functionalities of a firewall are to isolate environments, mask resources, filter incoming and outgoing data flows, and authorise (or not) the access to services. These can be performed by a separate information system (a hardware firewall) or by software (often a program running on a PC or server). Thus, a firewall is defined as a piece of hardware or software (or both) that allows the management of the data that flow across it by filtering them, according to parameters (criteria, filtering rules) defined during its configuration (Figure 12.18).

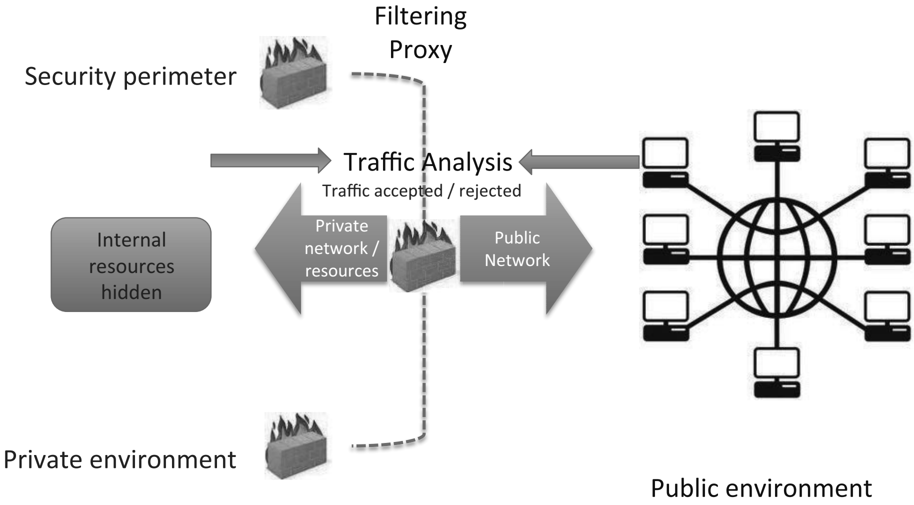


Figure 12.18 The Functions of a Firewall.

A firewall system helps to protect ICT resources by enforcing perimeter security. It acts as an intermediary device for internal and external connections, allowing the masking, separation, and isolation of resources. The main role of a firewall is to create a kind of security zone that allows certain entities to be separated and isolated, and to designate zones within which access to resources will be subject to specific control. The designation by a firewall of a security perimeter and a “demilitarised zone” (DMZ) isolates key systems and masks services. In order to do this, the firewall needs to support filtering, relaying, and masking technologies. The filtering function consists of analysing the communications through the firewall in both directions and can be implemented using a number of different protocols. The relaying and masking functions are usually associated with the "proxy" type of firewall, which masks the internal resources of the information system. Activity for each application passes through the proxy and requests for its resources are not sent to the application server directly but to the firewall, which passes them on. In the other direction, communications received from the Internet do not get routed directly to the internal systems but pass first through the firewall.

When installed judiciously as part of an organisation's network infrastructure, a firewall allows the reinforcement of the protection of internal systems by creating security perimeters. However, for such approaches to be really effective, organisations must identify very early the kinds of unauthorised access attempts that count as real intrusions into the information systems.

An *Intrusion Detection System* (IDS) helps to ensure the availability and integrity of resources and the confidentiality of data by avoiding, for example, the destruction, modification, and theft of data, the installation of Trojan Horses, and the hijacking of systems. It is difficult, however, to place total faith in the operation of IDSes because as a consequence of the way they work, they can be bypassed; no guarantees can be given for their absolute effectiveness. To ensure that they continue to meet requirements, it is fundamental to monitor the way they are working and to audit their logs so that their performance can be evaluated and any necessary changes made.

Although there exist a number of different types of IDS, none are completely effective. Even if firewalls and IDSes are useful tools in performing certain security tasks, they alone cannot guarantee the protection of IT resources.

Network Management as a security operational tool

One group of difficulties linked to making a telecommunications network secure comes from its nature and the way it works, specifically:

- the commonality, the sharing, the distribution of resources, and their accessibility at distance;
- the geographical coverage of the network (local to international);
- the way a network is instantaneous, dynamic and transparent and undergoes constant evolution;
- the number and diversity of the resources used and of the users;
- the intrinsic vulnerabilities of information systems;

- the way that management is split between various entities when networks from different domains interconnect (the difficult of providing a consistent end-to-end control framework); and
- the way that a public network is, by definition, open to the public, which is to say, open to entities that are benign or malevolent, without any automatic means of distinguishing between them.

These factors mean that this becomes a complex environment to control. Good network management, particularly including the management of configurations, performance, and incidents, helps ensure the availability and integrity of infrastructures, services, and data. In addition, the aspect of network management that refers to financial management allows the creation and maintenance not only of data to be used for billing users but also of data to be used for monitoring and auditing tasks – activities that are critical in the field of security. Such data can be used to verify the course of events, provide evidence of activities, or avoid repudiation if necessary. Network management also helps ensure the confidentiality of data in that it can prevent clandestine sniffing of, or unauthorised access to, data. The activity of controlling access to resources also falls under network management and is indeed fundamental to the operational implementation of security.

The availability of resources and services, a key security requirement, is dependent on the various activities related to the management of systems and networks (capacity planning, performance management, incident handling, etc.). The requirements for confidentiality and integrity can partially be satisfied by the implementation of access controls, by good server configuration, and by firewalls, all of which are activities covered by network management. Event logging, traffic monitoring, and incident detection are also activities that can be included in network operations and that contribute to improved security structures. In addition, the integration of the user helpdesk into the management of systems and networks can also contribute to greater visibility and coordination of security.

The management of IT installations begins with an inventory of the ICT and telecoms resources to be managed. Apart from the simple fact that only elements that are known can be properly managed and secured, such an inventor also contributes to the quality of configuration, performance, capacity, and operational management. Together these activities contribute towards meeting the requirements for availability, reliability, and integrity.

In addition, the inventory has a key role to play in the identification of resources to be protected, a process that is fundamental to all security planning. It provides the basis for a classification of resources based on their importance, criticality and the definition of the security measures deemed appropriate to protect them. The resource inventory also plays a role in the implementation of access controls, specifically in the area of defining access rights to resources based on users' profiles. The inventory thus contributes indirectly to ensuring confidentiality and integrity.

Monitoring a network involves continuously observing its performance. Network monitoring is not only intended to confirm that the quality of service is acceptable, but also to identify problems, incidents, errors, and anomalies that might degrade network performance and impact the security of resources so that timely and appropriate responses can be made. Network monitoring allows the traceability of activities and events so that they can be logged and subsequently analysed, both to find areas for optimisation and improvement and to find evidence of the causes of incidents. Network monitoring also contributes to the availability of resources by ensuring that the network is functioning properly. Thus, because it supports the management of performance, incidents, configurations, users, and security, it is an element of network management.

It is impossible to have security without quality management and without system and network management. At the same time there cannot be quality without security management, and for this, systems and networks need to be properly managed.

System and network management includes the installations and fairly technical procedures related to the operational security of network components. It is a part of the quality and the security of the whole organisation.

A pragmatic approach for effective and efficient security

Securing an ICT environment requires a pragmatic and coherent approach in which two complementary and inseparable knowledge bases must combine. These are:

- conceptual and organisational knowledge to be reflected in the definition and implementation of both a network management policy and a security policy;
- techincal and operational knowledge to be reflected in the implementation of effective solutions (such as products, mechanisms, and services for management and security).

Network administrators, like the people responsible for security, need to possess organisational skills (such as expertise in policies, procedures, activities, and in all aspects related to management), technical skills (in the use of tools), and human qualities. Essentially, they need to be capable of sharing, negotiating, and delegating, because a security system, regardless of how appropriate it might be, will only be useful if everyone within the organisation accepts it. This requires that the system is well distributed throughout the organisation and that the users who are aware of the impact of security issues understand it. Security is also a question of communication and of making users responsible for their conduct. Given that around 80% of accidents in businesses have an internal cause, simply making telecoms secure is not sufficient to protect sensitive assets.

When facing the dilemma of choosing the most relevant security solution out of a proliferation of proposed solutions in a context of the daily reality of security-related problems, the following questions are of relevance:

- Are the solutions adapted to the requirements?
- Can they be correctly installed and managed?
- Can they be used in, or adapted to, a dynamically evolving environment?
- Can they be used to address security problems that have their origins in negligence, human error, design flaws, installation problems, or the mismanagement of technology and security solutions?
- Can they mitigate the inordinate concentration of power in one position within the organisation?

The real operational information security challenge is to keep security handling simple and cost-effective. Security procedures and tools must be usable, effective, and efficient (Figure 12.19).

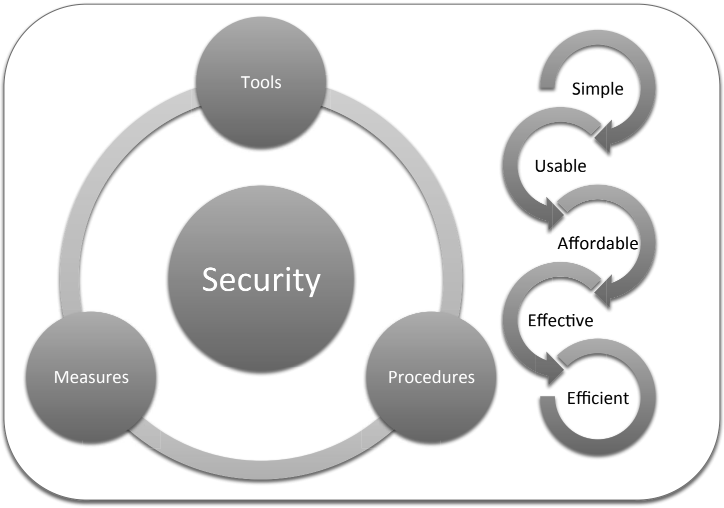


Figure 12.19 Summary of basic principles to be kept in mind.

Security needs must be taken into account right from the start when building infrastructure and considering accessibility. A minimum level of security for ICTs must be provided at an affordable cost.

Security depends on complementarity between the managerial, technical, and legal aspects that must be treated in parallel. It is never acquired definitively. The constant evolution of information systems and risks makes all security measures unstable. This finds expression in the problem of quality management that relates essentially to the maintainability and the development of systems, values, and risks. Security and quality approaches share the common goal of providing products and services for which the quality is guaranteed. Security must be approached in a global manner. Personal motivation, the implementation of measures, as well as the use of appropriate tools must be considered. It is important to insist on the fact that tools on their own cannot resolve administrative or managerial security issues. They are never a substitute for management. If disorganised and non-integrated within a continuous process, they can only hamper usage, load operations overheads, and degrade information system performance.

The security architecture reflects each of the dimensions of information security – organisational, legal, human, and technological – that need to be taken into consideration for a complete understanding of an organisation's security. The process of defining a global security architecture allows management to visualise the overall shape and the transverse nature of information security and to identify the various facets and components so that a consistent, complementary, and harmonious solution can be developed. This facilitates the integration of measures, procedures, and security tools.

Within the framework of a security architecture, it is also important to include the appropriate consideration of assets and risks, the respect of procedures, training and education, the ethical behaviour of users, and compliance with regulations. Security criteria can thus be met by the introduction of complementary measures and procedures.

Furthermore, the availability of an architectural framework provides a reference point for security that facilitates both the operational aspects of security and their evaluation when audited. This approach also identifies minimum security criteria for each component, as well as their interactions and any possible incompatibilities at different levels of security.

The design of a secure information system begins with the definition of the security architecture as a conceptual structure. This step is essential in a systematic approach that includes addressing the whole set of problems relating to system security and organisation so that a coherent and all-encompassing security strategy can be established.

12.6 Cyber security as a competitive advantage

While the monetary value of hardware is easy to assess, the value of data is far more difficult to quantify. Nevertheless, these very data provide the major part of the added value of the information systems. The enterprise's intangible assets and human resources form its real competitive factors.

In order to protect information, it is necessary to understand its role, its strategic importance, and its link to decision making, among other things. The level of protection required depends on the information to be handled. Establishing a preliminary classification of the data is also important, since it sets out its degree of sensitivity (normal, confidential, etc.). Thus, through using tables that relate the type of data to its degree of sensitivity, the number and nature of the logical locks to be applied can be identified. The approach evoked here is integrated into the implementation phase of security strategy. It is one of the aspects broached by the organisation's security policy. Logical security is not only a matter of the resource access control; dimensions concerning software development, application life cycles, and data quality should also be added to help define the security necessary for information and e-services that are accessible through telecommunication infrastructures.

Network security, the security over the software and hardware resources linked by the network, is also achieved by judiciously separating or isolating these resources from each other. It is equally important to secure the application infrastructure in which the applications are ultimately running (at the level of the user's work environment) and the applications themselves (by use of time stamping, origin validation, non-repudiation, and confidentiality procedures). Furthermore, application security should make it possible to ensure the user's privacy. Finally, for this secure edifice to be coherent and efficient, the security administration infrastructure must itself be secure. Telecommunications security alone cannot guarantee the security of electronic transfer. It is only one link in the whole security chain.

Providing a secure and robust communication environment requires securing all the elements in the information technology chain and processes. Moreover, telecommunication security cannot be envisaged without a prior specific risk analysis, as telecommunications permeate the enterprise's environmental, human, organizational, and information technology infrastructures. Implementing encryption mechanisms for data transfer, for example, without analysing other risks in the information system, cannot hope to solve an organisation's security problems. The organisation must first define a security policy that enables an inventory of all the relevant risks (and combinations of these risks) to the assets of the enterprise. At this point, the risks to be prevented can be identified and the appropriate preventive measures put into place.

Physical security represents the most fundamental and common control for information systems. Sensitive areas are not only ICT work and operations areas, but also those that house indispensable logistical equipment, such as electrical power supplies and air conditioning. With regard to logical security, physical controls only provide limited protection of data and resources. Identification, authentication, and access control processes to services and contents are of primary importance. At the same time, fundamental human rights must be respected so that business activities can be undertaken in a satisfying way.

12.7 Summary

At the systemic level, problems relating to ICT infrastructures and services security are similar to those of individual computer (system) security. They involve the same technical, organizational, and human requirements. Protecting information during its transfer is not enough. Data are as vulnerable, if not more so, when they are processed and stored. ICT security will be effective if homogeneous and complementary protection measures for ICT and resources and their physical environment can be set up.

Every institution needs to harmonize its usage and management procedures along with its legal framework. In addition, every user and contributor must be trained in security measures. Consequently, there is need for suitable educational programs and human resources management.

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 sheer negligence resulting from incompetence, misconceived or poorly implemented technology, excessive authority for system administrators, or mismanagement.

For organisations, the management of information risks consists of reducing them to an acceptable level. The border between acceptable and inacceptable risk is sometimes difficult to determine objectively and often depends on the organisation's objectives and on the context in which it operates.

Beyond the necessary dimension of security engineering, security is, above all, a management activity (the managerial dimension). The quality of security essentially depends on the quality of security management and on the quality of the staff responsible for it.

Information technology security is achieved through the rigorous management of logistics, human resources, information systems, networks, workplace sites, and environmental infrastructures (control of power supplies and natural risks) and by the respect of regulations and laws. Controlling information technology security is a management issue for which security tools and services are linked to the administration of operational systems. Tools, such as encryption and firewalls, cannot correctly ensure protection unless they form an integral part of a precise management process and are accompanied by procedures that govern their use.

It is of primary importance for organisations to achieve a sufficient level information technology security to minimise technological and informational risks. To do this, these risks must be correctly identified so that an appropriate security perimeter can be set up and assets protected effectively. Global security implies a multi-disciplinary and systematic management approach.

Considered as a system, telecommunications (infrastructures and services) security problems are not very different from those of individual computer security. Their resolution includes the same technical, organisational, and human requirements. Protecting information during its transfer is not enough, as data are quite as vulnerable, if not more so, when they are being processed and stored.

Information technology security will be effective if we can set up homogeneous and complementary protection measures for data processing and communication resources and also for their physical environment.

When considering purely technical aspects of security, it is necessary to link these technical measures to the effective implementation of operational and management procedures. In addition, the staff of the organisation must be trained in security requirement and measures; they must understand and respect them. For that, suitable human resources management is obligatory.

In the context of e-government or commercial applications, for example, it is especially difficult to manage end users because they are different and mostly unpredictable. Basic education and e-security public awareness plans, at a national level, need to be proposed.

Communications infrastructures must provide high performance and be secure to avoid being the weakest link of the information chain of e-applications. Pooling and sharing software and hardware resources, and information exchange supported by *n* actors linked to their transport and processing, must be integrated into a coherent strategic design policy for the development of an information society.

Under no circumstances should this introduce a degree of vulnerability. Insofar as states have made important efforts for the development of information and telecommunications infrastructure, it is essential that they provide their organisations and citizens with regulations, policy, and technological tools that enable them to carry out, manage, and be confident in their e-activities. This should be accompanied by a set of educational measures to develop and promote both a security-aware culture and ethical and responsible behaviour, and through investments in security research and development.

12.8 Exercises

1. What are the differences in meaning between the terms *cybersecurity*, *information security*, inf*ormation technology security*, and *information system security*?

2. Define the concept of the governance of the security of information technology.

3. What are the major differences between the governance and the management of information security?

4. What is the relationship between risk management and security management?

5. Why is the level of security in an organisation often the result of a compromise?

6. Describe the concepts of the strategic and operational dimensions of the security of information systems.

7. What are the ultimate goals of an information security policy within an organisation?

8. How can an information technology risk be defined, and what are the key elements of such a risk?

9. Can regulatory compliance contribute to improving information security within an organisation? If so, how?

10 What are the principal risks related to the outsourcing of all or a part of the information security activities of an organisation?

11. Why is the question of vocabulary important in the context of information security?

12. Why should information security be perceived as a continuous process?
13. What are the criteria of information security, and to what needs do they correspond?
14. What are the main functions of a PKI?
15. What is the purpose of a firewall?
16. What kinds of security services can be developed based on the implementation of cryptographic techniques?
17. How can the availability of data be ensured?
18. What are the main limits of access control methods based on biometric technologies?
19. To what extent do the characteristics of telecommunications networks make them difficult to secure?
20. Why do technical and technological measures fail to offer an absolute level of security?

Chapter 13

Cyberconflict & Cybercrime: Prospects for a Global Response

13.1 Understanding the context

The protection of information in an interconnected digital world is an issue for all of us. We are surrounded by technology from our births to our deaths. Digital technologies are a major factor in our civilisation and, whether we like it or not, digital technologies and the Internet have brought us firmly into the Era of Technocivilisation[1] (Figure 13.1). Information and communications technologies are everywhere; they are increasingly capable, increasingly invisible, but also increasingly intrusive. Telecommunications networks, using and including mobile telephone technologies, allow increasing access to communications, all the time, everywhere, with everyone but also with anyone.

The world today is complex, globalized, and, above all, dominated by the intensive use of ICT devices, infrastructures, and services. Citizens, organisations, and states are likewise increasingly dependent on ICT infrastructures for everything they need. It is a complex dependency with multiple interdependencies involving several types of actors distributed all over the world.

In parallel to society's increased dependence on technology, new forms of power are emerging. These forms of power are related to the ability of certain entities to manage and control digital technologies, cyberspace, IT infrastructure, and the security of all of these. Including the power for example, to

[1] Source: *"Technicivilisation: pour une philosophie du numérique."* R. Berger; S. Ghernaouti-Hélie. Collection Focus Science. PPUR 2010.

Technocivilisation
We are surrounded by technology from our births to our deaths
The world is complex, globalized and dominated by the intensive use and misuse of ICT

Figure 13.1 The techno-civilisation.

damage, to influence, to monitor, or even, to contribute to economic and social development, cyberpower can take many forms.

Nowadays trying to understand questions of cybersecurity cannot exclude due consideration of the ways in which mastering technologies and security can change both how power is distributed and how it is exercised.

Within this framework, and in order to contribute towards responding to the global need to manage cyber-risks and fight against cyberattacks and cybercriminality, thereby contributing towards peace, justice, and security in cyberspace and consequently in the physical world, we have been drawn towards identifying the need for a Global Treaty on Cybersecurity and Cybercrime.

13.2 Some complex and global questions[2]

Beyond geographical borders

The Internet, the most obvious element in cyberspace, does not recognise geographical borders. The only borders are those defined by technical or governmental filtering (and even these borders are trivial to cross, say the more expert Internet users). For example, there exist numerous sites containing content that is racist, anti-Semitic or neo-Nazi, run by French nationals, written in French and aimed at spreading propaganda on French soil and to French speakers.

[2] This section is an adapted translation of the chapter *"La cybercriminalité: Le cyberespace une valeur commune à protéger"* (p 775 – 904); S. Ghernaouti-Hélie, C. Aghroum – Rapport de l'Observatoire National de la Délinquance et des Réponses Pénales 2011 (ONDRP). Institut National en Hautes Etudes et Sécurité et de la Justice (INHESJ). CNRS Editions.

This kind of publishing is illegal in France, and such sites can easily be shut down if hosted in France or in a country with a similar legal framework.

However, it is not necessary to be hosted in some legally exotic country, as such sites can simply shelter in, for example, the United States. When confronted with a request to close a site, even a request that has been properly issued following the methods of international legal cooperation, the American government will reply by citing the First Amendment to the Constitution, a measure adopted on December 15, 1791, according to which freedom of speech is absolute.[3] Should American law apply to the whole planet when defining the proper use of the Internet?

But at the same time, the hosting of sites dedicated to, say, child pornography in other countries, such as Russia, which has not yet signed the Convention of the Council of Europe on the protection of children from exploitation and from sexual abuse,[4] demonstrates the difficulty in closing down such sites in such countries.

So other than filtering, what kind of solution can be adopted in a country that is aware of the limits of international law? Distinct from censorship, even if it is similar technically, such solutions can take the form in France of the blocking of child pornography sites, as provided for by Article 4 of LOPPSI II (Loi n° 2011-267 du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure).[5] This efficient measure designed to protect French Internet users, however, does not eliminate the source of the problem.

Without opening a discussion on the reasons behind this, it is worth noting that nowadays, it was easier legally to board a ship carrying drugs that is sailing on the high seas, by reference to Article 17 of the United Nations convention against the illicit traffic in narcotic drugs and psychotropic substances (Vienna, 20 December 1988),[6] than to block a single website containing neo-Nazi or child pornography materials.

[3] The United States Constitution – First Amendment "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances". Source: http://www.aidh.org/Biblio/Text_fondat/US_04.htm#1

[4] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No.: 201 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=201

[5] Law of orientation and programing for the performance of interior security.
Loi n° 2011-267 du 14 mars 2011 parue au JO n° 62 du 15 mars 2011.

[6] http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en

Beyond the idea of freedom

The idea of freedom is at the center of the debates on the future of the Internet. Three generations of users have participated in the creation of the modern Internet. The first used the Arpanet network, created by the military and used by researchers, and which was organised around consistent rules on discretion and security, protected by its isolation and unavoidable elitism, and open only to a small and limited brotherhood of users. The second was present at the opening of the Internet to the wider public, where users still remained bound by the same rules, requiring technical knowledge in an abstruse dialogue restricted to the initiated. Finally, the third saw the access permitted by the web, which has allowed an Internet open to everybody that has become by philosophy a medium for free exchange, a new territory beyond the reach of the police and customs officials. Entering this fourth dimension does not involve crossing any visible frontiers, even if the space is at the same time restricted by national sovereignty and an area where such restrictions can easily be avoided. There are codes of conduct for airspace and the seaways, but there is no unanimously accepted code for traffic on the Internet, where freedom is the key principle that allows all kinds of fantasies, the choice of a new identity, and to make one's way, hidden or masked. The arrival of blogs and social networks has liberated egos and welcomed new experiences, either under the user's real name or under a fictitious identity. Everyone can now have the feeling of being a journalist, a photographer, critic, novelist, sound engineer, cameraman, or editor.

Very quickly the confidential online space created by the pioneers was invaded by profit-seekers, rapidly followed by those seeking to extract profits from illicit activities, hidden from legal consequences, protected by the ease of anonymity provided by digital technologies and the access to tools that, until then, had been restricted to the intelligence services and the military (such as monitoring technologies and methods of encryption).

The Internet user, both a creator and consumer of the Internet and its related services, is becoming a hostage in the clash of cultures (ancient versus modern, east versus west, north versus south, democracy versus dictatorship). The user is active in an area that is considered by some to be a simple medium for exchange, by others to be a huge shopping centre, and by still others to be a playground or a battlefield where conflicts can be played out. At the crossroads where these often contradictory uses meet, and in the absence of a global authority to regulate activities, the Internet can be a place of freedom. This dream is mere illusion, however, in totalitarian regimes that limit the freedom of expression on the Internet by implementing filtering.

Beyond the digital web

Although the Internet is a source of knowledge, culture, and exchange, is also a source of disinformation and propaganda, easy to produce for the same reasons as the truth is easy to publish. All the necessary tools are easily available: software to re-touch photographs, editing software, scanners, and formatting tools. The Internet is particularly suited to the transmission of rumours, urban legends, false accusations, and simple lies because there is no right to forget and because the fascination created by the media often leads to a lack of common sense on the part of the Internet user, who is ready to believe whatever he wants to hear. In the absence of a trusted third party, everyone chooses a desired identity: perfect for playing or teasing, impressive for cheating or corrupting. The twelve-year-old girl is actually a habitual paedophile (this is known as *grooming*). The supposedly trustworthy banking site is actually a fake site designed to acquire the identities and credit card details of Internet users who have been tricked (this is *phishing*). The brilliant company director and the beautiful but lonely foreign lady are in fact crooks who make contact in order to pick up a few thousand Euros through seduction or playing the charity card…

As a medium based on anonymity (and thus a dream tool for criminals and terrorists), the Internet can also be used for propaganda, proselytising, and remote and discreet exchanges. What is a drugs network or a separatist of ideological organisation if not a hierarchical grouping of correspondents scattered around the world who use new technologies for their own purposes? States and public authorities that rely on their intelligence services and judicial systems need to be able to explore, monitor, control, and even restrict the use of the Net.

In parallel, tools are being developed for searching, social engineering, and business intelligence that dig ever deeper into the Internet, crawling around and bringing to the surface, in a structured way, a huge quantity of information, merged and cross-referenced, that destabilizes rules of privacy and private lives. Soon, more information will be available in open sources than in police files. This is already the case for honest people, about whom state services, in reality, actually know little, and far less in any case than large businesses actually do.

In favour of the regulation of digital exchanges

It can be understood from the preceding discussion that the use of the Internet can no longer, even in democracies, be left to users and service providers to govern. It is no longer an enclosed, private space, but rather a public area subject to the authority and control of individual states within the confines of their national sovereignty and in accordance with international agreements. Constraints will thus be applied progressively in order to protect the Internet user from himself and from others. The analogy with the Highway Code is trivial, but it nevertheless illustrates the phenomenon: in the early days of the motorcar, a code was unnecessary because of the small number of vehicles on the roads, and the few motorists could manage the roads with a mixture of courtesy and common sense. Nowadays, the freedom to drive is subject to a code that defines the rights and responsibilities of everyone and is accompanied by methods of ensuring that the code is respected. The use of the Internet will follow the same path. The various means of blocking access to child pornography sites that have been implemented by the majority of western countries demonstrate clearly that the need for the regulation of digital exchanges has been recognised.

A compromise is required, a compromise by which cyberspace is guaranteed to be both free and protected, secure so that every user can freely exercise his basic rights without hindrance, a place for exchanges, a place of knowledge, of culture, of leisure, and of business that is sheltered from the Big Brother gaze of governmental, intergovernmental, commercial, or criminal groups. It could be a space where one behaves according to codified rules, recognised by everyone except the criminal fraternity, with territorial and extra-territorial zones that are clearly defined and subject to arbitration and recognised international authorities that are recognised by all. Article 28 of the Universal Declaration of Human Rights declares: “Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.” Why shouldn’t this order apply to cyberspace? In a world that is subject to the law of information and communication technologies and an international treaty on cyberspace, the last two paragraphs of Article 29 of this Declaration should be implemented.

The UN already possesses, in its founding charter of June 26, 1945[7], a tool for controlling and administrating international conflicts that can be extended to cyberspace. Chapter VII: “Action with Respect to Threats to the Peace, Breaches of the Peace and Acts of Aggression is relevant to current times and can be easily applied to cyberconflicts. Let us imagine – as a case study – a denial of service attack by one country on another, aiming to block its governmental communications or trade exchanges. The application of Articles

[7] http://www.un.org/en/documents/charter/index.shtml

41 and 42[8] is just as legitimate as in the case of a more traditional military attack.

The military aspects, so frequently at the centre of the debate around cyberspace – for the same reason as games and the sex trade are the catalysts for the development of the media – have allowed the creation of areas of research that have rapidly been identified and analysed. The correct ordering of all the domains – civil, penal, commercial, legal, cultural – can only be envisaged in the framework of an international treaty.

13.3 For an international treaty: a contribution to stability in cyberspace

The origins

The proposal for "A global treaty on cybersecurity and cybercrime: a contribution for peace, justice and security in cyberspace" [9] is framed in a perspective of the durable development of the information society, of the management of the risks created by the extensive use or misuses of digital technologies, and of information security at the service of individuals, organisations, and states. It has emerged from a long period of international co-operation of which the origins could be found in the work that the present author undertook with the Norwegian judge Stein Schjolberg within the framework of the International Telecommunication Union (ITU)'s *Global Cybersecurity Agenda.* In 2009 Judge Schjolberg and the author published a first proposal for an international treaty in the form of a book, the second edition of which appeared in January 2011. By way of background, the ITU launched in May 2007 the Global Cybersecurity Agenda (GCA)[10] for a framework within which the

[8] **Article 40** "In order to prevent an aggravation of the situation, the Security Council may, before making the recommendations or deciding upon the measures provided for in Article 39, call upon the parties concerned to comply with such provisional measures as it deems necessary or desirable. Such provisional measures shall be without prejudice to the rights, claims, or position of the parties concerned. The Security Council shall duly take account of failure to comply with such provisional measures."
Article 41 "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."
Source: http://www.un.org/en/documents/charter/chapter7.shtml

[9] The book, *A global treaty on cybersecurity and cybercrime : a contribution for peace, justice and security in cyberspace*, Stein Schjolberg, Solange Ghernaouti-Hélie can be downloaded from: www.cybercrimedata.net

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

international response to growing challenges to cybersecurity could be coordinated. In order to assist the ITU in developing this strategic proposal, a High-Level Experts Group (HLEG) was established. More than one hundred members of this group were nominated by ITU Secretary-General, with due consideration to both geographical diversity and range of expertise, to ensure multi-stakeholder representation. Judge Stein Schjolberg from Norway was the HLEG's Chairman.[11] In this context November 2008 saw the delivery of "The Global Strategic Report" [12] that includes recommendations on legal measures, technical and procedural measures, organisational structures, capacity building, and international cooperation.

The ITU Global Cybersecurity Agenda provides the essential architecture to set up effective national and international measures to encourage countries to develop national cybersecurity programmes and international co-operation. It should be seen as an important first step towards a global cybersecurity approach.

Of course, the rules of ethics, good behaviour, and good practices are as important in this domain as they are everywhere else. Nevertheless, good intentions of all kinds, like all non-binding recommendations, are of little use when confronted with:

- the political and economic stakes related to the management of cyberspace and digital technologies;
- the realities of the criminal world; and, above all,
- the fact that cyberspace should be considered as a universal asset.

Protection of a shared asset

Whether it is a case of delinquency, major criminality, or economic terrorism, information and telecommunications infrastructures form both the target and the means of committing crimes. In relation to power struggles, the search for profits, intimidation, threats, takeovers, destruction, surveillance, the manipulation of information, money laundering, and a variety of other activities, information technologies and cyberspace are now key factors in carrying out crimes, acts of terrorism and of war, both economic and non-financial.

[11] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/foreword_chair.html

[12] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
Moreover, ITU had created in 2008 the International Multilateral Partnership Against Cyberthreats (IMPACT). "IMPACT is an international public-private initiative dedicated to enhancing the global community's capacity to prevent, defend and respond to cyberthreats" (www.itu.int/osg/csd/cybersecurity/gca/impact_index.html).

In order to avoid cyberspace becoming solely an economic and military battlefield that reflects various kinds of conflicts or competitions of an economic or political nature, it will be necessary to view it as a common domain, the fifth after the land, the sea, the air and space (Figure 13.2). Cyberspace, like the other domains, has a great need for coordination and co-operation among all nations. It will require means of coordination and cooperation and effective legal measures at the level of every country. Thus a supranational controlling body, within the framework of the United Nations, widely recognised at the international level and effective at the national level, should be created.

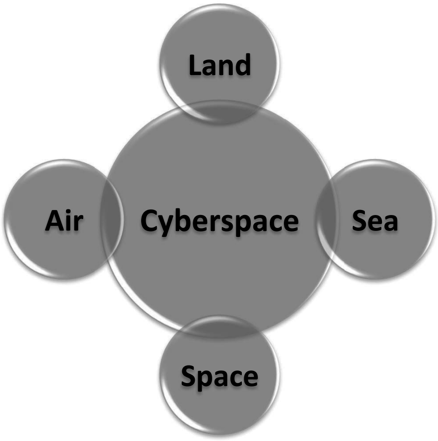


Figure 13.2 Cyberspace: the fifth common domain.

This should also contribute towards avoiding the abuses arising from a dominant position, reducing risks and threats, specifying which practices are and are not acceptable, and proceeding against offences regardless of where they were committed. In addition, it should contribute to a greater understanding of the needs for prevention, leading to an increase in the level of robustness and resilience of infrastructures, avoiding security breaches, minimising weaknesses, and anticipating undesirable events.

There is a real and urgent need for an international agreement, for a coherent and global approach to deal with cybersecurity and cyberattacks issues. Organisations, businesses, and states face significant risks in relation to the inappropriate disclosure, misappropriation, and destruction of data and information, and such incidents, when viewed at a macroscopic level, can be viewed as posing a potential threat not just to the competitiveness or reputation of a business but also at a national level to public safety, national security, or democracy itself.

These issues cannot be addressed effectively on a purely local level. In the same way as the Kyoto Protocol is an international agreement linked to the United Nations Framework Convention on Climate Change, a Global Protocol on Cybersecurity and Cybercrime should be seen as a truly global approach to reducing risks and threats in cyberspace. It should provide the essential architecture for setting up effective national and international measures to counter cyber attacks, and should include the clear definition of acceptable and unacceptable behaviours, and of the frameworks necessary for control.

About conflict issues

Hacking has become a weapon. Many kinds of people can hack into critical information infrastructures, such as criminals who want to blackmail the owners of a system, terrorist groups, or even mercenaries or government agencies wanting to generate chaos in another country through cyberspace. If their goal is to disturb and disrupt, hacking is an excellent way to reach it. Hacking is developing into such a powerful weapon that it is forcing us to rethink the concept of conflicts between states.[13]

Cyberwarfare, defensive, or offensive computer warfare – whichever name is used – involves economic and/or military conflict, and raises, among others, the question of individual, national, global, and international responsibilities, the question of international collaboration, and the question of private and public partnerships.

In any case, national and international strategies should exist not only to respond to cyberattacks, thus defining reactive measures to be undertaken after an attack, but should also consider proactive measures in order to avoid security breaches and to prevent unsolicited incidents. This could be done, for example, through developing an appropriate cybersecurity culture and diplomacy, by reducing vulnerabilities that could be exploited to attack systems; in fact, strategies should systematically consider all factors that can lead to, for example, deviant behaviours, crises, acts of retaliation, or crimes, and thereby enhance complementary and coherent measures in a holistic and global way.

[13] To give only one example, consider Israel and Palestine. Representatives of both sides hack each other on a daily basis. No amount of security is going to stop some of these hacks from being successful, because both sides are incredibly motivated. Without resolving the root of the problem – the conflict between the two states –the relentless hacking cannot be stopped.

The need for an international instrument

Cyberspace can be increasingly considered as a global economic and military battleground, where all kind of cyberconflicts can arise, reflecting every kind of political and economic competition. Thus, it is time to define what is acceptable or not on a common and approved basis and to set up an effective international instrument for controlling this. Without a common understanding and an international agreement, it will be impossible to set up effective security measures to correctly protect ICT resources (including critical information and vital infrastructures), to fight against cybercrime, and to preserve fundamental Human Rights.

Without a strong commitment between all actors and relevant stakeholders at national and international levels, it will be impossible to address cybersecurity needs at national and international levels. An international agreement should facilitate the development of a global strategy to deter cyberthreats from any direction. The process of working towards a United Nations Treaty should help develop a common understanding of all aspects of cybersecurity among countries at various stages of economic development.

All stakeholders need to come to a common understanding of what constitutes cybercrime, cyberwarfare, and other forms of cyberthreats. This is a prerequisite for developing national and international solutions that harmonise cybersecurity measures. These kinds of common understandings will also help to reduce the divide between the perceptions of cybersecurity in developed and developing countries. Because criminal conduct in cyberspace is global by nature, it requires the global harmonization of cybercrime legislation; it requires effective international justice and police co-operation and a genuine will to accomplish this (Figure 13.3).

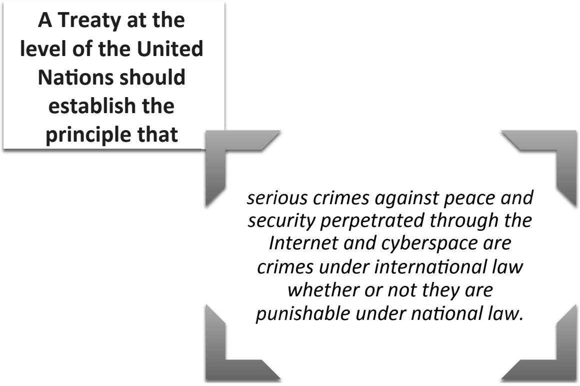

A Treaty at the level of the United Nations should establish the principle that
serious crimes against peace and security perpetrated through the Internet and cyberspace are crimes under international law whether or not they are punishable under national law.

Figure 13.3 A global treaty.

A Global Treaty at the level of the United Nations should establish the principle that serious crimes against peace and security perpetrated through the Internet and cyberspace are crimes under international law, whether or not they are punishable under national law. The most serious crimes in cyberspace should be defined and handled under international law.

Regional agreements are not enough

Nevertheless, the Council of Europe Convention on Cybercrime (2001), ratified on July 1, 2004, was an historic milestone in the combat against cybercrime. This Convention constitutes only one example of a regional initiative, and many countries have preferred to make use of the Convention as a reference and nothing more, because it is, and always will be, a European convention. In other words, it is necessary within a global framework, at the level of the United Nations, to establish a treaty or a set of treaties including the broadly accepted standards and principles in the Convention, but with certain important additional provisions.[14]

Countries outside Europe should use the Convention as a guideline or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal systems and practices with certain exceptions and additional provisions.

The emergence of international debates

Since 2009, we have presented the framework of an international treaty related to cybersecurity and cybercrime at several international events and conferences and to UN agencies, such as, for example, the Internet Governance Forum IGF-2009, the *United Nations Congress on Crime Prevention and Criminal Justice* in El Salvador – 2010, the ITU Global summit on the information society (WISIS 2010, 2011) around the world.[15]

The initiative has also been the subject of many scientific and wider-audience publications and has resulted in numerous interviews with different media, both national and international.

[14] Some countries do not accept some standards and principles, especially the principle in Article 32 of the Convention on cross-border access to stored computer data with consent or where publicly available. Those countries must be respected for their opinions (Source: Chairman's report HLEG, ITU 2008).

[15] in USA, Japan, China, Brazil, Switzerland, Norway, France, Egypt, the United Kingdom, Israel, Singapore, Ukraine, etc.

At the moment we are working with the East-West Institute (EWI),[16] an international think tank where a Cybercrime Legal Working Group, chaired by Judge Schjolberg, and of which the author is a member, was created in 2010. The group has the objective of advancing discussions of a treaty or a set of treaties on cybersecurity and cybercrime. The members are independent, non-political, non-governmental experts in these fields working on recommendations that will promote co-operation and serve the global community.

The EWI Cybercrime Legal Working Group[17] members are independent global experts from all continents. The group develops recommendations for potential new global legal mechanisms for cybersecurity, cybercrime, and global cyberattacks, as well as a consensus-building set of proposals related to international law at the level of the United Nations. The goal of the Working Group is to make proposals for non-partisan, objective, non-political solutions that may promote collaboration and serve as a potential compromise for the global inter-governmental organizations. The five main subjects, or pillars, addressed are:

- international criminal law for cyberspace;
- a global virtual taskforce for investigation and prosecution;
- an International Criminal Tribunal for Cyberspace;
- cybersecurity issues;
- blocking of child pornography websites; and
- online child abuse.

At the same time two other global working groups, the UNODC group and the US-EU group, are currently working on the same kinds of issues, defending the idea of a Global Convention on Cybercrime. Moreover, in 2011, UNODC (United Nations Office on Drugs and Crime) and ITU signed a Memorandum of Understanding, "United against Cybercrime."[18] This partnership focuses particularly on capacity building related to cybercrime.

As previously mentioned, the Internet and cyberspace have become, at a global level, components of the civilisation that we will leave to future generations as part of their heritage. For this reason, it is our duty and our responsibility, both individually and collectively, to determine together the common values that we wish to promote and see respected internationally.

[16] http://www.ewi.info/

[17] The text related to the EWI Cybercrime Legal Working Group was written by Judge Stein Schjolberg (Norway), chairman of the Working Group.

[18] http://www.unodc.org/

It will take time to build a cyberspace, the security and reliability of which we can rely upon, and this project will require many kinds of resources and skills. Such a project will be based not only upon dedicated technologies and management procedures and a specific legal framework that is enforceable nationally and compatible at an international level, but also upon means of governance and control that are recognised and verifiable internationally.

These means will need to be developed and implemented with, and to the benefit of, all the participants in the global use of the Internet, with a particular input from the giants of the Internet that contribute so much to its success. Certain fundamental principles must also be identified, adopted, and widely recognised by the international community, following the example of the Universal Declaration of Human Rights in 1948[19] (Figure 13.4).

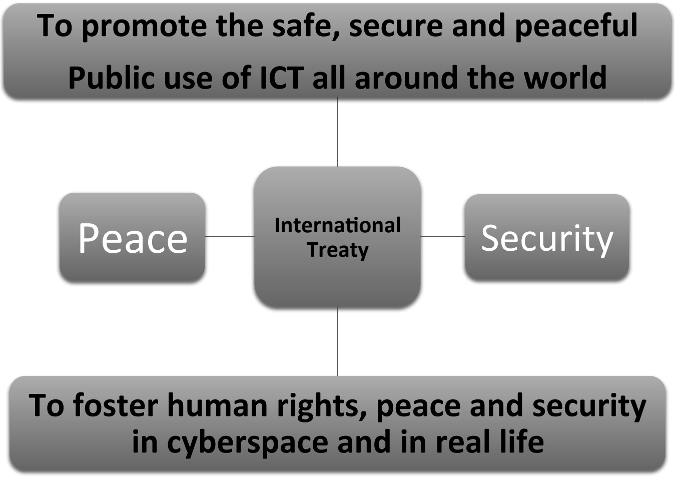

To promote the safe, secure and peaceful
Public use of ICT all around the world
Peace
International Treaty
Security
To foster human rights, peace and security in cyberspace and in real life

Figure 13.4 Some fundamental principles.

It will not be a simple matter to define successfully these commonly accepted values, given the differences in countries, cultures, and economic and political stakes. The creation of a global treaty on cybersecurity and cybercrime will doubtless be a long process. This is why it is urgent to start now to implement a mechanism that will facilitate an international dialogue, so that it will be completed in a timeframe that corresponds to the global stakes.

[19] http://www.un.org/en/documents/udhr/

Even bearing in mind the difficulties confronting the creation of such a treaty (which of course might well not be respected, as the earlier example of the Universal Declaration of Human Rights illustrates), it would constitute an instrument to be deployed against bad behaviour, be it by individuals, organisations, or states. As a result, it should contribute towards avoiding a drift away from common values, or at least highlight divergences, and allow, where appropriate, compensation through legal channels.

During the Second Worldwide Cybersecurity Summit in London in June 2011, Sir Michael Rake, the Chairman of British Telecom Group, stated that it was "critical to try to move towards some sort of cybertechnology non-proliferation treaty."[20] This comment reflects the same need for the international community to find solutions that will allow cyber-risks to be restricted to an acceptable level.

This could prove to be insufficient, however, as it reduces cyberspace and information technologies to the status of tools of the military world that could be used as weapons. But the frontiers between the military and civilian worlds are not clear; the same technologies are used and the Internet is the same for everyone, from the very youngest to the most senior users, for economic development, for massive fraud, for cyber-espionage, or as cyber weapons.

The 1968 Treaty on the Non-proliferation of Nuclear Weapons,[21] a treaty the benefits of which are no longer under discussion despite continued difficulties in its application, serves as an analogy; this treaty was of no use in preventing the nuclear catastrophe at Fukushima in March 2011, which was not the result of military actions. On the other hand, an organisational structure such as the International Atomic Energy Agency (IAEA)[22] has shown its value in the co-ordination of the monitoring of the catastrophe and in the creation of the security measures, which followed it. Applied to cyberspace, an equivalent

[20] Associated Press "Web summit considers cyber-nonproliferation pact" By RAPHAEL G. SATTER, 06.01.11, 01:17 PM EDT, http://www.forbes.com/feeds/ap/2011/06/01/technology-telecommunications-no-b-cybersecurity-summit_8494580.html
The Associated Press June 1, 2011, 2:39PM ET AP Interview: US says no new treaty needed
By PAISLEY DODDS. Bloomberg Businesssweek
http://www.businessweek.com/ap/financialnews/D9NJ8ET02.htm

[21] Treaty on the Non-Proliferation of Nuclear Weapons. Opened for signature at London, Moscow and Washington on 1 July 1968 http://www.un.org/fr/disarmament/instruments/npt.shtml
(UNODA United Nations Office for Disarmament Affairs : http://www.un.org/disarmament/
UNIDIR – United Nations Institute for Disarmament Research http://www.unidir.org/html/en/home.html)

[22] "The IAEA is the world's center of cooperation in the nuclear field. It was set up in 1957 as the world's "Atoms for Peace" organization within the United Nations family. The Agency works with its Member States and multiple partners worldwide to promote safe, secure and peaceful nuclear technologies." Source: http://www.iaea.org/

structure should exist to promote the safe, secure, and peaceful public use of information and communication technologies.

This analogy to nuclear weapons and power stations (which is, to be honest, both daring and limited) should not cover up the need to implement a global and holistic approach to addressing the problems relating to cyberspace security, problems that justify the adoption of a treaty (or a collection of treaties) that recognises both the military dimension and all others. Cyberspace is of benefit to all kinds of criminals whose activities, such as money laundering or human trafficking, for example, will have impacts on both the military and civilian domains. But even above these specific considerations, is it acceptable that Human Rights are not respected in cyberspace?

A global treaty (or a set of treaties) on cybersecurity and cybercrime at the level of the United Nations would contribute to more peace, justice, and security in cyberspace and in real life.

For a sustainable development approach

The following generic questions should be taken into consideration when thinking of cybersecurity in terms of a sustainable development approach. Is public order compatible with social insecurity?

How could measures that are solely technological, inert, and seldrem followed by sanctions ever be effective over the long term? Any technical security solution is merely a tool used within the framework of a larger program. It would be a mistake to simply apply technologies unless in response to a clearly identified need.

There are still more questions without ready answers. At this very moment, who is actually controlling security? Those who are directly concerned by the need for security or those who provide solutions and services? Is it those who use and offer services on the Internet, or is it rather those who know the weaknesses and understand the techniques for exploiting those weaknesses? Those who create security code or those who are capable of breaking it? Civilians, the military, the intelligence services, commercial businesses, ISPs? Those who design, manufacture, and sell electronic equipment (including processors) and software, or those who are capable of reverse engineering?[23]

[23] Reverse engineering – techniques allowing the recreation of source code based on the examination of an executable programme.

Who has the authority and the legitimacy to control the Internet and provide new impetus? The countries of the northern hemisphere, the strongest economically, or those countries whose linguistic power is starting to shift the centre of gravity of the Internet? According to the International Telecommunications Union (ITU). One inhabitant in three of this planet is now connected to the Internet, and contrary to a widely-held ethnocentric idea, for the last three years developing countries have been creating more Internet users than developed countries.[24]

These questions remind us that confidence in the IT and telecoms infrastructures on the part of all the different providers and users will be drawn from the knowledge of risks and of the people responsible for managing these risks. This confidence will benefit everyone. In particular, this is why information security and surveillance products need to be transparent and auditable by, or on behalf of, their users. It is on this basis that the security market will gain recognition and achieve a level of maturity that corresponds to the stakes. Information security, which can include monitoring, will thus become the cornerstone of the success of information technologies that serve everyone. The idea of service providers, including security service providers, holding users (individuals, organisations, or states) hostage is no longer acceptable.

13.4 Connecting the world responsibly

"Connecting the world responsibly" was the slogan at the World Internet Governance Forum (IGF) that took place in Egypt in November 2009. This slogan, which we can surely all agree upon, may represent more of a utopian vision than the reality of the Internet world. Poverty and social exclusion are closely linked and have caused many people to be left behind in every country. Unfortunately, the development of information society has not brought any major changes. The Internet may reach into all corners of the globe, but some people are still excluded from the global village. What we call *the digital divide* (where people do not have access to communication and information technologies) is often the sign of a social gap that also raises issues such as illiteracy, even in developed nations.

And while the Budapest Convention on Cybercriminality was celebrating its tenth birthday on November 23, 2011, the anniversary will only have

[24] Source: measuring the information society 2012. www.itu.int/ITU-D/ict/publications/idi/index.html

been noticed in some fifty countries.[25] This is regrettable, as it is in the widest possible interest to implement measures designed to manage the risks of the inappropriate disclosure of information, the illicit acquisition of resources, or the hijacking of information and communication technologies, including coordinated attacks on critical infrastructure. These risks should be considered at a macroscopic level as potential threats to competitiveness, to the reputation of institutions, to state sovereignty, to national and public security, and, ultimately, to democracy itself.

The adoption of a cyberspace treaty, and the implementation of measures for control and follow-up to ensure that the treaty is respected, would contribute to connecting the world in a responsible way. This will not be enough, however, if the question of personal data protection is not satisfactorily addressed at the international level. In the world of information, all digital activities leave a trace. Some users know how to mask or delete these traces; others know how to collect them, correlate them, extract them from their original context, or otherwise manipulate them. Although Internet users are responsible for what they publish about themselves and about others, for example on social networks, everything is geared towards encouraging them to communicate ever more information: personal data, behaviours, tastes, geographical locations, habits. Cyberspace is not free, and when a service is described as free, its users pay in kindly providing their personal data.

Nowadays, an enormous quantity of personal data is stored across the Internet, a situation that has given birth to the concept of Big Data. This does raise, with some urgency, the question of the risks being run by people who cannot master, use or protect these data.

By way of analogy, half a century ago asbestos was *the* solution for insulation purposes. Asbestos was thus applied extravagantly. Nowadays, everything is being done to remove asbestos wherever it is found, with the costs being borne by society as a whole and by those who suffered from its effects. Today, everything is being done to get people to connect and consume Internet services, but tomorrow will it be possible to disconnect from Facebook and Google, for example, and at what cost? Recognising the hidden facets of information technologies, such as security technologies, so as to be able to predict their long-term effects, is a complex exercise that very few decision-makers are capable of performing. The use of social platforms reveals in some a need for exhibition that should not be confused with a need for transparency, and a need for the application of monitoring that is undergone and implicitly accepted.

[25] http://conventions.coe.int/treaty/EN/Treaties/Html/185.htm

The foreign correspondent Claude-Marie Vadrot[26] reminds us of the phrase of Felix Dzerzhinsky, the founder of the Soviet KGB: "the only people who fear surveillance are those with something to hide." This phrase has come back into fashion in a context where, contrary to long-lasting principles, every citizen is now fundamentally viewed as a suspect. Thus as increasing hyper-surveillance is imposed upon us, the authorities try to convince us that we are all under threat from "the others," that "the other" is both an enemy and the object of permanent curiosity, and that we need to be totally transparent.

Today, some businesses take possession of large amounts of personal information from their customers, without the overview of an independent body. Often users are not informed that their data is being used, or to what purpose, or even if they have consented to it. Similarly, personal data protection – therefore individuals themselves – may become threatened if, for example, in a context of national security strategy against crime and terrorism, collaboration takes place between governments as well as with service providers.

Personal data can be considered commercial or trading assets in some countries where legislation for the protection of personal data is lacking. An important number of large Internet companies, such as service and social networking platform providers, take advantage of this situation to develop their economic models. They can make large profits through commercialising and exploiting personal data, which users have either given freely or which has been collected without their knowledge. However, lawful players in the marketplace are not the only ones involved in data use; criminal organisations, and even isolated individuals, know how to obtain personal information illegally and use it to maximise their profits or reduce their own risks.

In general the major players on the Internet, both private and public, view the need for the protection of personal data and for the respect of digital privacy as being risks with a potential negative impact on the business or on security – rather than being fundamental rights. This ignores that the protection of personal data is a precondition for self-determination and for the protection of the freedom of expression and human dignity. It is written into the universal declaration of human rights, and contributes towards stronger democracy, greater social justice, and a decrease in discrimination and violence.

[26] Source: Claude–Marie Vadrot. Extracted from "Trop de sécurité engendre l'insécurité. La surveillance et la vidéo surveillance remèdes placebo au malaise social," a presentation given during a public conference on "Les droits de l'homme au regard d'internet et de la sécurité informatique: Posture ou imposture?" at the University of Lausanne on December 3, 2009. C-M. Vadrot is most notably the author of "La grande surveillance" (Seuil 2007).

Connecting the world in a responsible way should include, among other things, respecting fundamental rights, processing personal data honestly, and not using such data for purely commercial purposes or for the creation of general-purpose files. These objectives can be achieved if the operation of systems is in compliance with the following legislation and regulations (among others):

- the guidelines of the Organisation for Economic Cooperation and Development (OECD) regarding the protection of privacy and the international transmission of personal data (September 23, 1980);
- the Convention of the Council of Europe for the protection of individuals regarding the automatic processing of personal data (January 1981);
- the European Convention on Human Rights (ECHR) from 1998, Article 8, which stipulates the right to respect one's "private and family life, his home and his correspondence"; and
- Resolution 45/95 of the General Assembly of the United Nations of December 14, 1990, whereby the governing principles for the regulation of electronic files containing personal data were unanimously adopted.[27]

Without yielding to the ideology of fear, fear of ecological risk, or fear relating to public order, it is essential that a real public debate takes place, not only around questions of the increasing reliance of society on information and information systems, but also on the related subjects of the security of citizens, organisations, and states, all within a world of generalised interconnections. Information security must be understood in a context of a global society and in a holistic way that will permit a realistic equilibrium between the needs for and requirements of protection, between the assurance of individual and collective interests, and between the sovereignty of individual states and the needs of international collaboration, all the while respecting the fundamental rights of all humans. These points should logically form a privileged basis for the development of an information society.

With this in mind, the major players on the Internet, both public and private entities, have a duty to suggest security solutions that address technical, legal, and financial issues and are both realistic and convincing, solutions

[27] References:
http://www.oecd.org/document/18/0,3343,fr_2649_34255_1815225_1_1_1_1,00&&en-USS_01DBC.html
http://conventions.coe.int/treaty/fr/Treaties/html/108.htm
http://www.echr.coe.int/echr/fr/header/the+court/how+the+court+works/archives/travaux.htm
http://huwu.org/french/documents/instruments/docs_fr.asp?year=1990

that mean that liberties are not exchanged for an illusion of security and that, when necessary, the work of the justice system and the police can be effective without damaging fundamental liberties. These security solutions should not lead people to forget that such measures alone cannot protect against injustice. It is essentially deceptive to make people believe in a technological and security-based mirage, to promote obligatory and generalised surveillance as an unquestionable asset, and to train consumers and those being managed to adopt a docile pattern of behaviour. This final point gives legitimacy to the removal of liberties as soon as no countermeasures exist. In this respect the independence of the CNIL in France,[28] and of its equivalent members of the Group of 29 in Europe,[29] is fundamental.

What cannot be allowed to happen is that security is performed in secret by public administrations or private entities. Security is essential, but we need to know who is in charge of the security and who is watching the watchmen. This is part of the reinvention and the reappropriation of the concept of net neutrality, in which the need to combat criminality and the requirements for respecting individual liberties are integrated. It would be judicious to mobilise the combined abilities and knowledge of IT, security, and legal professionals, of politicians, and of citizens in this movement in order to learn from and inform them of their responsibilities regarding the requirements for security and the increased importance for society of information systems. Thus, it is essential that reliable and convincing long-term security solutions exist and can be used by the public, so that the situation of exchanging liberties for ineffective protection can be avoided. The idea of being able to protect human rights in terms of technologies and security requirements presupposes the existence and availability of information, debates, realistic alternatives, and a real willingness on the part of all of the concerned parties. Beyond simplified

[28] The Commission nationale de l'informatique et des libertés (CNIL) is responsible for ensuring that information technology remains at the service of citizens, and does not jeopardize human identity or breach human rights, privacy or individual or public liberties. The Commission fulfils its duties in pursuance of the law of January 6, 1978, as amended on August 6, 2004. Source: http://www.cnil.fr/english/the-cnil/

[29] Advisory working party created by Article 29 of Directive 95/46/CE.
The Article 29 Working Party is composed of representatives of the national data protection authorities (DPA), the EDPS and the European Commission. It is an important platform for cooperation, and its main tasks are to: (1) provide expert advice from the national level to the European Commission on data protection matters; (2) promote the uniform application of Directive 95/46 in all Member States of the EU, as well as in Norway, Liechtenstein and Iceland; and (3) advise the Commission on any European Community law (so called first pillar), that affects the right to protection of personal data.
Source: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Cooperation/Art29

ideas of good and evil, between paranoid fantasy and naïve mythology, information security needs to be developed in a framework of transparency and sincerity.

13.4 Summary

The Internet, the network of all networks, is an excellent way of getting in touch with people and making contacts. It contributes to the spread of knowledge, to social and economic development, and, if nothing else, it can be a way of enriching personal life. However, it is also an instrument of power, a marketplace where everything can be bought and sold, and a tool that allows the development of digital surveillance on a very large scale. Cyberspace is not purely virtual. It represents a vision of the world with a political, economic, and social reality.

The important increase in large-scale computerized surveillance is due to the widespread use of SIM cards, smart cards, telephones, GPS systems, Internet, and RFID (Radio Frequency Identification), etc., all of which leave digital traces. This contributes to potentially threatening several human freedoms: the freedom of speech, the freedom of association, the freedom of movement (the right to travel and to navigate freely on the Internet), the right to knowledge and information, and the right to respect for private life, family, and correspondence.

It is no simple task to define common values that are acceptable regardless of country, culture, and political and economic stakes. Defining an International Treaty on Cyberspace is a long process. This is why it is urgent to immediately implement a mechanism for facilitating an international dialogue that will conclude within the proper timeframe for such global stakes as those raised by the control of cyberspace.

Even conscious of the difficulties inherent in the process for obtaining such a treaty (which, by the way, might simply not be respected, as can be shown by the example of the Universal Declaration on Human Rights that has already been cited), such a document would remain despite everything a *binding instrument* applicable to all deviant behaviours, be they by individuals, organisations, or states. Because of this it should anticipate deviations or, at the very least, highlight them and obtain reparations, if appropriate, through legal channels.

Whether it is a case of delinquency, major criminality, or economic terrorism, then, information and telecommunications infrastructures form both the target and the means of committing crimes. In relation to power struggles, the search for profits, intimidation, threats, takeovers, destruction, surveillance, the manipulation of information, money laundering, and other activities, information technologies are key factors in carrying out crimes, acts of terrorism and of war, economic or otherwise.

To protect cyberspace from becoming solely an economic and military battlefield that reflects various conflicts or competitions of an economic or political nature, it will be necessary to view it as a common domain, the fifth after the land, the sea, the air, and space. As is the case for these domains, cyberspace will require means of coordination and cooperation and effective legal measures at the level of every country. Thus, a supranational controlling body, within the framework of the United Nations, widely recognised at the international level and effective at the national level, should be created.

This should also contribute towards avoiding the abuses arising from a dominant position, reducing risks and threats, specifying which practices are and are not acceptable, and proceeding against offences, regardless of where they were committed. In addition, it should contribute to a greater understanding of the needs for prevention, leading to an increase in the level of robustness and resilience of infrastructures, avoiding security breaches, minimising weaknesses, and anticipating undesirable events.

13.5 Exercises

1. What is the primary means of combating cybercriminality on a global scale?
2. What are the major points justifying the creation of an international treaty on cyberspace?
3. What would be the advantages and limitations of an international treaty on the non-proliferation of cyberattacks?
4. Explain in what ways an international treaty on cyberspace could contribute to stability and peace both in cyberspace and in the real world.
5. Why are regional agreements insufficient in the context of the struggle against cybercriminality?
6. What have been the benefits of the GCA (Global Cybersecurity Agenda) promoted by the ITU (International Telecommunication Union)?
7. Can cyberspace be considered as a universal, shared asset?

8. Based on the Universal Declaration of Human Rights (http://www.un.org/en/documents/udhr/), identify the fundamental rights that can be infringed or denied in cyberspace.

9. Why must digital privacy be protected?

10. Why is it problematic to consider personal data as yet another kind of commercial asset?

11. What does the expression, "connect the world in a responsible way," mean to you?

12. Outline some ways in which an approach based on durable development can be applied to the Internet and cyberspace.

13. Suggest a definition of the concept of *technocivilisation* and what it encompasses.

Glossary of main cybercrime and cybersecurity related terms

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 gather 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 Virus-detection programme.

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 computerrelated attacks.

Attacks against critical infrastructure An attack targeting specific infrastructures such as electric power supplies, nuclear power facilities, water supply schemes, etc.

Attack tool An attack tool is an automated script (programm) 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 order to meet requirements (no denial of authorized access to systems, services, data, infrastructure, etc.).

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.

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 door 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.

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, 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.

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.

Computer crime Theft of computer services, unauthorized access, software piracy, alteration, 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.

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.

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.

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.

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.

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.

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.

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).

Cookies Files written to internet users' hard file without their knowledge, when they access certain websites, and that collect data on the users with a view, in principle, to customizing the web services offered.

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.

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 digital environment 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 Appeared after September 11th, cyberterrorism is a kind of terrorism utilizing cyberspace to attack critical infrastructures.

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.).

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 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 service) 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.

Eavesdropping This term originally referred to simply listening to a conversation, but now it has taken on digital implications. The interception of e-mail, 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 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.

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, encipherment 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. Moral value systems are systems of principles governing morality and acceptable conducts.

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.

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.

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.

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.

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 'black hat' activities and analyze potential system weaknesses. Honeypots can also provide an environment for post-attack forensic analysis.

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.

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.

IPSec (Internet Protocol security) A version of IP 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*, builtin mechanisms for implementing security services (authentication of source and destination entities, confidentiality of transported data).

ISO 17799, ISO 27001 Information security management standards set by the International Organization for Standardization.

Jurisdiction The right of a Court to make decisions regarding a specific person (personal jurisdiction) or a certain matter (subject matter jurisdiction).

Key Encryption or decryption key, usually a mathematical value for 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.

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.

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, messages between two parties without either party knowing that the link between them has been compromized.

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.).

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.

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.

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 semm 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.

Protection The act of protecting or the state of being protected. Protection is said of a security measure that helps detect, neutralize or reduce the effects of an attack.

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.

Quantum cryptography Quantum cryptography uses quantum mechanics to secure communications. At present, quantum cryptography is only limited to secret key distribution.

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.

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. Watermarking is a steganographic application that consists in placing indelible marks on an image.

Surveillance Continuous monitoring.

System intrusion The entry of an external and unauthorized person or software into a system.

Threat 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.

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 Assured reliance on someone or something (a qualitative, subjective, highly relative criterion).

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.

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.).

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.

Zombie
A system that has been hijacked by a hacker and utilized (without its owners' knowledge) to send spam or malicious codes.

Annex
Some references

Some ICT Security issues websites

http://www.itu.int/cybersecurity/
ITU (International Telecommunication Union) activities related to cybersecurity

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 (November 2005)
www.oecd-antispam.org - OECD toolkit on spam

Some related Internet-law issues websites

www.cybercrimelaw.net - 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.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
www.rsf.org/ - Reporters Without Borders

Some computer-crime-related issues websites

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp
Council of Europe website dedicated to cybercrime and actions against economic crime

http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
Interpol website dedicated to fight against cybercime

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

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)
http://www.weforum.org/ - The World Economic Forum portal on cybersecurity and cyber resilience's issues
http://www.ewi.info/ - The EastWest Institute portal on cybersecurity's issues

Book resources

Inside Cyberwarfare, Jeffrey Carr, O'Reilly 2009. Case studies that help understand the cyber underworld.

Cyberpower and National Security, edited by F. Kramer, S. Starr, and L. Wentz, NDU Press 2009. Perspectives related to national security in United States

Cyberwar: the Next Threat to National Security and What to do About it, Richard Clarke and R. K. Knake, ECCO Press of Harper Collins Publishers 2010. Discusses the risks related to cyberwar in United States.

War 2.0. Irregular Warfare in the Information Age, Thomas Rid and Marc Hecker, Praeger Security International, 2009. The book explores how the Web 2.0 and more precisely the uses of social networks could lead to political insurrections.

Strategic Warefare in Cyberspace, Gregory J. Rattray, MIT Press 2011.

Surviving Cyberwar, Richard Stiennon, Goverment Instituted (UK) 2010.

Cybercrime: Criminal Threats from Cyberspace (Crime, Media and Popular Culture), Susan W. Brenner, Praeger 2010.

Understanding and Managing Cybercrime, Sam C. McQuade, Pearson 2006.

Computer Evidence, Collection and Preservation, Christopher L.T. Brown, Course Technology – Cengage Learning 2010.

Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Course Technology 2009.

Hackers: Heroes of the Computer Revolution, Steven Levy, O'Reilly 2010.

Forensic Computing: A Practitioner's Guide, Tony Sammes and Brian Jenkinson, Springer 2007.

Social Engineering: The Art of Human Hacking, Christopher Hadnagy, Wiley Publishing Inc. 2011.

The Art of Deception: Controlling the Human Element of Security, Kevin D. Mitnik, Wiley Publishing Inc. 2002.

CYBER POWER

CRIME, CONFLICT AND SECURITY IN CYBERSPACE

Solange Ghernaouti

Today, cyberspace is where new forms of criminality are being exploited; and cyberspace has become the economic and military battlefield where conflicts of all kinds are played out. The ability to control information and telecommunication infrastructure, to respond to cyberattacks and to ensure cybersecurity offers real power and has become one of the most significant political, economic and technological issues of this twenty-first century.

Information and communication technologies (ICT) have grown to become a critical part of our society's infrastructure, and their potential misuse affects us all, from the individual citizen to private and public organizations and states. Thus cyberpower has become the newest means for organisations – both legitimate and criminal – to demonstrate their capabilities.

This book explains the stakes of cyberpower in terms of its various manifestations, including cybercriminality, cyberterrorism, cyberconflicts and cyberwarfare. It evaluates the impacts on, and consequences for, individuals, organisations and states. It provides a panorama of the actors and their means of operating and describes the strategies, methodologies and kinds of measures that can be employed to combat the abusive and criminal uses of digital technologies, and thus improve security within cyberspace and in real life. The book's educational approach, including numerous illustrations, exercises and case studies, makes a complex subject accessible to a wide public.

Professor in the Faculty of Business and Economics of the University of Lausanne, SOLANGE GHERNAOUTI is a pioneer and an internationally recognized expert on cybersecurity and cybercrime-related issues. Her main focus is on developing an interdisciplinary, integrative and practical approach to cybersecurity – one that is useful for citizens, organisations and states. She is a frequent contributor to media discussions of security matters and has participated in initiatives organized by the International Telecommunications Union, the United Nations and the Council of Europe. She is a member of the Swiss Academy of Engineering Sciences (SATW) and has been recognized by the Swiss press as one of the most influential women in professional and academic circles.

G16840
ISBN-13: 978-2-940222-66-7
9 782940 222667

EPFL Press

CRC Press
Taylor & Francis Group

N10719
ISBN-13: 978-1-4665-7304-8
9 781466 573048