Department of Impresa e Management

Master Degree in Consulenza Aziendale

Thesis in Competition and High-Tech Markets

CRITICAL ATTACKS: HOW ECONOMY COULD BE SAVED BY CYBER INSURANCE

TUTOR

Professor Andrea Renda

CO-TUTOR

Professor Francesco Rullani

CANDIDATE

Eleonora Bianchi

ID 651901

Academic year 2013/2014

INDEX

Chapter four

The impact of cybercrime on security

Chapter five

The economics of cyber insurance

LISTS OF FIGURES AND TABLES

INTRODUCTION

Nowadays, it is consolidated the large and massive use of the Internet and its applications, causing more and more structures to be laid upon the Internet and its interconnections; it goes from simple users, that surf the Net for searching general information and social interactions, to business users, that rely on the Internet for economic and working issues, to administrative users, in this group stand large and important users like they can be banks and financial institutions and governments.

The heavy and important dependence of society on information technology implies that valuable and key assets are potentially and easily exposed to global cyber threats, and furthermore that any users can be susceptible to cyber attacks, paralysing their operative terms and leaving them exposed to further damages (A practical guide to assessing your cyber security strategy, 2012). Cybercrime has become a "*silent, global and digital epidemic*" (Symantec, 2010), many worldwide victims tend to feel powerless and unprotected against "*faceless cyber criminals*" (Symantec, 2010) Cybercrime has significant side effects that can be financial or not, and that involve much more layers than just few years ago, because of stronger and deeper interconnection of the Internet.

For thus, this outlines the need of employing cyber security measures, which consist of "*a combination of technology and security procedures*" (U.S. Department of Homeland Security, 2013). Many layers are involved in the construction of a suited security combination. Applying cyber security is the first step of security combination, it consists of technologies, processes and practices designed to protect networks and data from attacks, damages and unauthorized access; however, since attackers are always one step further and can exploit any kind of vulnerabilities in the system, cyber security cannot prevent all potential attacks which networks are exposed to.

So, there is need to check out security confidence, through cyber assurance, that systems are confident enough to meet both operational needs (Alberts et al., 2009), and stress situations like attacks, failures, accidents and unexpected events. In this case, it is helpful to prepare a disaster plan, according to strategic risk management, that can be activated in case of cyber attacks. At

the same level, there is information assurance that comprehends operations of protection and defence of information systems by ensuring and controlling their availability, integrity, authentication, confidentiality, and non-repudiation, including the restoration of information systems by incorporating protection, detection, and reaction capabilities. It consists essentially of systematic protection throughout acquisition, elaboration and storage of information and data.

As last step of combination, companies arrive to cyber insurance in order to transfer risk to other parties. Cyber insurance has as purpose to mitigate losses caused by cyber accidents. Its main goal and benefit is to sensitively reduce number of cyber attacks thanks to preventive measures that discourage them. The fundamental mechanism of insurance applied to IT is the encouragement of implementation of best practices, by basing premiums on the level of self-protection adopted by insured party (U.S. Homeland Security, 2012); in this way insurance can limit the level of losses faced during and after a cyber attack.

Therefore, the principal hypothesis this thesis is aiming to answer to is that cyber insurance can effectively be a vital tool and strategy for firms, in particular for critical infrastructures owners and operators, in order to mitigate all those risks that cannot be covered and absorbed by cyber security strategies implemented by companies. Indeed, the major objective of the dissertation is to highlight the significant role of critical infrastructures and to encourage cyber security with more than one approach and strategy.

Cyber insurance has been described as "an *effective, market-driven way of increasing cyber security*" (U.S. Department of Commerce, 2011). In fact, it is nearly impossible to reach a perfect coverage by attack and damages. This impossibility is due to several causes (Pal, Hui, 2012). First of all because there is not yet sound and proven technical solutions, secondly because of the varied intentions that lay behind attacks, but also misaligned incentives between network users, security providers and regulatory authorities leave room for attacks; there are strong externalities and free-riding problems, moreover it is difficult to measure quantitatively and qualitatively risks; system failure is

amplified by customer lock-in and first mover effects of vulnerable security products and by problem of lemons market, which is the electronic medium of computers networks, "*via which online communications takes place*"(Pal, Hui, 2012).

In this failing system, cyber insurance is catching on, according to Pal and Hui, thanks to three reasons. It increases the overall network safety by adopting self-defence strategy, in order to respond to an increase to insurance premium. Cyber insurance integrates the partial protection offered by cyber security strategies; in fact, these means cannot reach absolute protection unless it upgrades technologies and it should face enormous expenditures to adequate security systems. Therefore, it is an optimal choice to transfer risks, faced because of lack of total security, to a third party that can leverage them. Cyber insurance, moreover, can be a solution to misaligned incentives, by combining benefits that actors seek on the Internet. Insurers earn profit from premiums, network users will be able to hedge potential losses, while security software producers can benefit from first mover advantage and lock-in strategies.

Even if sure data is missing regarding breaches and attacks, because of credibility and image companies' purposes, it is possible to have a look at the insurance market, thanks to the increased number of purchased cyber insurance. 70 % of companies that have suffered in the past two years a cyber attack or cyber damages are more conscious of cyber insurance and more interested in it. According to Marsh (Marsh, 2013), purchase of insurance increased 33% in 2012; in fact, highly visible attacks and the increasing awareness of cyber risks and their possible costs are growing, leading the market to think cyber insurance as an essential purchase for business. This, moreover, has made insurance more affordable also to small and medium enterprises (Marsh, 2013), that, otherwise, would have been excluded by benefits of insurance, even if possible target for attacks.

According to a recent survey conducted by Ponemon Institute, the phenomenon of security incidents and data breaches costs multimillion dollar losses to business. Data breaches go to "simple" negligence or mistakes that cause the loss of confidential information, to real cyber attacks that cause disruption of

operations, like denial-of-service attacks, or even damage to IT infrastructure. Consequently, insurance prices swing depending on size and risks faced by company's computers. Standard policy covers risks in collecting data and property and revenue losses resulting from network failures (Katz, 2013-b). Therefore, the average price can range from $5,000 to as high as $25,000 or $35,000 per $1 million worth of coverage.

The principal assumption on which this dissertation is relying is the importance and criticality of critical infrastructures, that, consequently, need further and more focused protection against both physical failures and damages and, especially, cyber-related attacks. Nowadays, all the world rely on a well-functioning Internet, for any kind of services, from transportation to energy, from health care to energy, from food to government. The "*interconnectedness within and across systems also means that infrastructures are vulnerable to local disruptions, which could lead to widespread or catastrophic failures*" (National Research Council, 2002). The stronger the interconnection between users, infrastructures and security, the less resilient is the system made by critical infrastructures. When an infrastructure provides vital and fundamental services to the nation's well-being, which comprehends state-of-art functioning systems, security and public order within national borders, it is called critical infrastructure.

European Council formulated the Directive 2008/114/EC of 8th December, 2008, which establishes common procedure for identification and designation of European Critical Infrastructure (ECI). ECI is defined as "*critical infrastructure located in the EU Member States, the disruption or destruction of which would have a significant impact on at least two Member States of the EU*"(Holt, 2013). The list of Critical Infrastructures is growing at an increased pace. The most important macro areas are Finance and Banking, Manufacturing, Food and Agriculture, Health, Energy, Water, Transportation and Postal services, Security and Emergency services, Government and Information and Communications Technology.

So, the threat of "*catastrophic terrorism*" (National Research Council, 2002) has given a new meaning to government-private relationship, for integrating

security issues with daily business decisions. In fact, there must be set a clear and effective cooperation among government and private companies in order to maximize the security over critical infrastructure and minimize costs and disadvantages that can arise during a not-efficient collaboration, which can create obstacles to the final objective, which is protecting critical infrastructures.

First of all, incentives must be put clear and motivating for private companies in order to undertake all the necessary actions for reducing infrastructure vulnerabilities; often it is more convenient from a business point of view to accept the risk of an hypothetical or possible terrorist attacks or damages than coping with sure costs, that tend to outweighs the future benefits. Even if government can set goals, it lays on private companies to efficiently implement steps, because they have deep knowledge of the overall system. However National Strategy for Homeland Security (2002) represents an obsolete approach to the problem, where government addresses protection activities only to markets that do not provide adequately on their own. The strategy assures that there are enough and enough strong incentives in private market to supply sufficiently protection, ensuring to rely on private sector. Even if numbers agree with this statement, as 85% of critical infrastructures is privately owned, it is consolidated that a backup support of government is essential, since "*market forces alone are, as a rule, insufficient to induce needed investments in protection*" (National Strategy for Homeland Security, 2002).

Despite a lack of incentives for private companies, large corporations have political and financial forces and credibility to assume the role of protecting infrastructures, moreover they have, or at least they can afford, technical expertise and experience. However, they face uncertainties because of asymmetrical information, as other critical infrastructure tends to retain information about their own infrastructures, and therefore, they can underestimate the emergency behind protecting critical infrastructures.

It is evident that securing critical infrastructure, in order to win back growing and evolving cyber threats, is requiring a layered and cooperative approach. There must be strong and active cooperation between public and private sectors

to prevent, protect from, respond to and coordinate mitigation efforts against attempted disruptions and adverse impacts to national critical networks, like cyber, communications and infrastructure, and major hazards, like terrorism and natural disasters. U.S. Threat Assessment (2013) brings to attention the increasing risks that face critical infrastructure, that at the same time erode economic outputs and national security. The required pace of necessary improvement in cyber security needs to be fostered and accelerated in order to meet rapidly the increasing risk of cyber attacks and espionage.

There is a growing overlap of private company over intelligence agency, "*it's sort of like a mini-CIA at the organizational level in order to understand where the attack is originating from*" (Katz, 2013-a). Other organizations that cannot afford such efforts in intelligence, tend to cooperate with government in order to help its intelligence to model an efficient attack. When a cyber deterrence takes place, private companies can easily respond to cyber attacks, acting like cyber attackers, inside and outside national borders, thanks to the cooperation with telecommunication companies. What this situation highlights is the anarchic regime that rules the Internet. Even if a company has the power to counterattack a potential cyber criminal in another part of the world, does it have the legal right to attack first? In fact, it is a situation of private users, even if powerful and endorsed. If it is government, it rules warfare, Congress in 2012 authorized Pentagon to "*conduct offensive operations in cyberspace to defend our Nation, Allies and interests*"(U.S. Congress, 2011), *i.e.* to use the most effective way to deal with threats and protect U.S. and coalition forces by undertaking offensive military cyber activities. But, when it comes to private corporation, it is different and more complex, as it should be.

"America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

(U.S. President Obama, February 2013)

From these words, it is possible to see how insurance offers benefits and incentives to invest in cyber security, by providing lower premiums for those that take appropriate precautions against cyber attacks. Cyber insurance can increase level of self-protection and the overall Internet security (Lelarge, Bolot, 2009).

Cyber insurance can be used to induce firms and private companies to adopt risk-mitigating behaviour (Sheety *et al*., 2010). For this, cyber insurance is "an *extremely promising route to solving the identified market failures in software security*" (Hahn, Layne-Ferrar, 2006), but it needs also backup coverage insurance for other level damages. Essentially, cyber insurance can protect, placed side by side with classic insurance, computers and IT systems from human errors or attacks, network damages, data breaches and much more. Cyber insurance is an instrument for encouraging investments in cyber security. Cyber insurance must be helped with an improved data flow about attacks in order to estimate damages, to increase awareness of problems about cyber risks and to make competitive the cyber insurance market.

In conclusion, this thesis will aim at proving and explaining that cyber insurance market is essential and a vital presence for companies that want to transfer cyber risks to third parties. In special way for critical infrastructures, cyber insurance represents an effective and efficient tool in order to encourage owners and operators to implement improved cyber security strategies and it reassures stakeholders of the reliability and resilience of these backbone structures, which are assumed to continue providing their services for the sake of society well being.

This thesis is structured in five main chapters, which face principal topics and issues related to critical infrastructures and cyber insurance.

Chapter one rotates around the figure of critical infrastructures and their interdependencies with the external environment, formed by society, economics and politics. Through a deep and transversal theoretical investigation, it is possible to notice how critical infrastructures are fundamental and essential for the entire world.

Chapter two investigates in critical infrastructure particularities which are Critical Information Infrastructures. These are the base of many other critical sectors, linked with strong interdependencies and nebulous boundaries as Internet and telecommunications technologies (ICT) improve and enter daily life with numerous and different applications.

Chapter three deals with the importance and value of information and data, which constitute the essential raw material for any business. As WikiLeaks has proven, the security and protection of sensitive information and data becomes a priority for organizations, which try to construct valiant models that could help business to deal efficiently with everyday operations and processes. Therefore, models and management strategies would be useful and indispensable for business in order to handle carefully these key assets.

Chapter four shows the risks that organizations, and general users, meet by using and running IT infrastructures, which represent the pivotal structure for modern organizations. In fact, cyberspace and computer machines are now the key platform in which the complex relation between human factors and economic advantage takes place, as the Internet and its infrastructure connect people, provide governmental services and help running businesses and services. However, the complexities are evident for any users, since risks, threats and vulnerabilities are the first threat to organizational security, and it also represents one of the top threats to national security, second only to terrorism.

Chapter five introduces the importance of cyber insurance, which transfers cyber risks to an insurance company that can effectively and profitably mitigate risks in return of premiums. In fact, as the importance of the Internet grows, firms are more vulnerable to threats and risks coming from cyber criminals, who attempt to gain unauthorized credentials and access to sensitive information, causing significant financial and business losses to firms. However, cyber insurance proves that, if effectively implemented alongside with cyber security strategies and risk management procedures, it is a valid ally for mitigating those risks that remain uncovered by normal security strategies. Moreover, cyber insurance may affect positively other industries and users, thanks to improved cyber security spread over the Internet and IT infrastructures.

Chapter 1

CRITICAL IMPORTANCE OF CRITICAL INFRASTRUCTURE

Chapter one rotates around the figure of Critical Infrastructures and their interdependencies with the external environment, formed by society, economics and politics. Through a deep and transversal theoretical investigation, it is possible to notice how critical infrastructures are fundamental and essential for the entire world.

In **Understanding criticality of Infrastructures**, it goes through the characterization of critical infrastructures, giving all-around definitions and appointing differences of notions among different countries, in order to see how these infrastructures are peculiar to nation's mindset.
This is going to represent the basis for any other consideration made upon critical infrastructures, since from the definition originates different approaches.
Then, it is going to analyse the actual status of critical systems, and the aim is to provide a holistic view of the ongoing situation. This can help to understand the connections at the base of the complex web created by interdependencies among infrastructures, which represent the tool over which shock transmissions are propagated to numerous international infrastructures. An overview of status of principal infrastructures, like electric power system and information and telecommunication networks, helps to understand the real importance of these, and the meaning of a possible failure or downturn and consequences in everyday life .

In **Economic and Political Considerations** it is faced another aspect of critical infrastructure, in order to give full representation of their importance. Policy has the duty to prepare proper strategies in order to better embrace structural, financial and organizational issues that are essential to make function infrastructures. The balancing of prevention actions and mitigation strategies

should be addressed not only from engineering point of view, but also from policy-making mechanisms that can ensure a better protection and resilience of these vulnerable systems.

In **Coping with Malfunctions**, the chapter ends highlighting the importance of assessing a proper protection of infrastructures through steps and strategies, which will be useful before, during and after the event that will cause the failure or the damage. The partnership among government and private sector is essential in order to ensure the right and fair investments for protecting infrastructures. Moreover, thanks to a small gallery of cases in which malfunctions are present, it is possible also to have a look to what had been done and what would have been done better, in order to lower costs and risks, also to human life.

Chapter 1

CRITICAL IMPORTANCE OF CRITICAL INFRASTRUCTURE

1.1 UNDERSTANDING CRITICALITY OF INFRASTRUCTURES

1.1.1 DEFINITION OF CRITICAL INFRASTRUCTURE

Infrastructures is defined as "*basic facilities, services and installations needed for the functioning of a community or society*" (The American Heritage Dictionary of the English Language, 2000*);* represent nodes and networks in the background that are necessary to put into action events or certain actions. For this, infrastructures work in the shadows and basically disappear from users' consiousness, that understand infrastructure importance and their dependencies on this backbone, especially during failures or breakdowns. New infrastructure can emerge rapidly and easily, but it can face naturalisation process and thus can be taken for granted in everyday life (Dodge, 2008).

"Users tended not to worry where the electrons that power their electricity came from; how their telephone conversations (or later faxes and Internet messages) were flitted across the city or the planet; how complex technological systems sustained their journey to work; or what distant gas and water reserves they were utilizing in their homes"

(Graham, 2000)

Infrastructures, thus, have become more and more important for civilized economies and also developing countries' economies; efficiency and risk management are primary objectives to pursue with adequate policies and strategies. All users rely on groups of "*interlinked physical and information infrastructures*" (Hammerli, Renda, 2010) that can perform daily requests and operations. These assets are essential for the correct functioning of society and overall economy. In the latest decades, infrastructures both physical assets and networked environment are a constant and important piece of everyday life. The infrastructures become progressively more interdependent in good and bad

luck. Moreover, in a globalised world, infrastructures can produce cross-border effects (Hammerli, Renda, 2010). So failures and reaching minimum resilience standards level have side effects spread over users and geographical regions, as in the case of massive energy blackouts in 2003 spread all over USA, Canada[1] and Italy.

Interdependency and importance of these infrastructure are the focus for economy, government and social life, therefore there are infrastructures considered critical, since their malfunctioning and failures can bring a general disturbance or, worse, to a loss of investments, efficiency and life comfort.
Each nation has defined in a peculiar way critical infrastructures and has outlined guidelines for discerning them from non-critical ones. In general, critical infrastructures are characterized by a strong dependency on each other and also interdependency (Hammerli, Renda, 2010); an example can be Information and Communications technology is dependent on Energy infrastructure, and, in the meanwhile, it is interdependent with many others critical infrastructures, like Finance, Government and also Energy itself. It is important to identify and prioritize which part of backbone is the most essential to its major duty or the most significant in order to avoid malfunctions, or which part may create danger or threat if damaged. Starting from a correct definition, it is possible to construct around a proper and effective security strategy; in fact, an unclear understanding of criticality of these infrastructures, because of their intrinsic complexity, can bring to inefficient solutions of policies and of investments addressing.

In U.S., critical infrastructure topic has been analyzed and ruled since a first report of Congressional Budget Office in 1983. It defined what an infrastructure is, that means "*facilities with the common characteristics of capital intensiveness and high public investment at all levels of government. They are, moreover, directly critical to activity in the nation's economy*" (in Moteff, Parfomak, 2004). New attention was brought to this topic in the mid-1990, when threats of terrorism were growing. In 1996, Executive Order 13010

[1] "Power System Outage Task Force — Final Report on the 14 August 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004, [http://emp.lbl.gov/sites/all/files/2003-blackout-US-Canada.pdf] [19th February, 2014]

defines infrastructure, starting from 1983 definition, "*the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defence and economic security of the United States, the smooth functioning of government at all levels, and society as a whole"* (in Moteff, Parfomak, 2004). This new definition prioritizes particular infrastructures over others on the basis of national importance, claiming that "*certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defence or economic security of the United States*" (in Moteff, Parfomak, 2004). At that period, the list of Critical Infrastructures includes Telecommunications, Electrical power systems and Water supply systems, Gas and Oil storage and transportation, Banking and Finance, Transportation, Emergency services, like medical assistance, police and rescue, Continuity of Government. In a Presidential Decision Directive in 1998, it has been introduced the goal of protecting critical infrastructures from intentional disruption and attacks and it has been expanded toward cyber infrastructures, as essential systems as physical infrastructures. The list goes wider after terrorist attacks, including more systems and infrastructure to be protected, it includes energy supply chain and critical facilities, other utilities, special events of national interests, telecommunications, nuclear sites and its supply chain, public and privately owned information systems, transportation by air, water and land, including airports and civilian aircraft, agriculture and systems for provision of water and food for human use and consumption. Patriot Act passed in 2001 opened the way to a stricter control and punishment against terrorist attacks that take place in USA but also around the world and to a comprehensive law enforcement of investigatory and surveillance tools. So forth, in 2002, it has been issued National Strategy for Homeland Security (NSHS), that lists more completely critical infrastructures comprehending Agriculture, Food, Water and Energy, Public Health and Emergency services, Government and Defence, Transportation, Information and Telecommunications, Banking and Finance, and it added to the list Chemical industry and Postal and Shipping, because of their increasing economic value and importance. NSHS states the distinction among cyber and physical

infrastructures. Department of Homeland Security is in charge of protecting cyber infrastructures and also key assets, which are monuments or represent symbols or historical attractions. U.S. definition of critical infrastructure has evolved over time and it has included more and more sectors, which became eventually critical for economic and civil welfare.

In table 1.1 it is shown the evolution undertaken by numerous U.S. executive orders that step by step have covered more and more critical infrastructures sensitive to government, whose aim is to protect them and ensure they are well-functioning for society sake.

Table 1.1: Evolution of U.S. Government Reports and Executive Orders protecting Critical Infrastructures during years

Infrastructure	U.S. Government Reports and Executive Orders					
	CBO (1983)	NCPWI (1988)	E.O. 13010 (1996)	PDD-63 (1998)	E.O. 13228 (2001)	NSHS (2002)
Transportation	X	X	X	X	X	X
Water supply /waste water treatment	X	X	X	X	X	X
Education	X					
Public health	X			X		X
Prisons	X					
Industrial capacity	X					
Waste services		X				
Telecommunications			X	X	X	X
Energy			X	X	X	X
Banking and finance			X	X		X
Emergency services			X	X		X
Government continuity			X	X		X
Information systems				X	X	X
Nuclear facilities					X	
Special events					X	
Agriculture/food supply					X	X
Defense industrial base						X
Chemical industry						X
Postal / shipping services						X
Monuments and icons						X
Key industry / tech. sites						
Large gathering sites						

Source: in Moteff J., Parfomak P., Critical Infrastructure and Key Assets: Definition and Identification, CRS Report for Congress, 2004

In Europe, critical infrastructures are defined by European Commission as a system or part of it situated in a member state that is essential for continuing vital social functions and that the disruption or damages would have a significant and strong impact on a member state (Council Directive 114/2008). European Critical Infrastructures (ECI) are those infrastructures of the highest importance for the Community and, if a failure or a disruption occurs, it would affect two o more member states if critical infrastructure is located in another

member state. So the criteria for identifying eligible critical infrastructures are: be placed in one member state; its functions are vital for society, like ensuring health, security, economic and social well-being; a possible failure can damage significantly a member state.

Considering what it has been said about both United States and Europe, it is useful to notice correspondences and differences among these two models of defining critical infrastructures.

Table 1.2: Different sectors included in US and EU Critical Infrastructures policies

Critical Sectors - American Government	Critical Sectors - European Commission Proposal
Food And Agriculture	Food
Water and Wastewater Systems	Water
Dams	Research Facilities
Healthcare and Public Health	Health
Nuclear Reactors, Materials and Waste	Nuclear Industry
Emergency Services	Space
Information Technology	Information, Communication Technology (ICT)
Energy	Energy
Transportation systems	Transport
Financial Services	Financial
Chemical	Chemical Industry
Communications	
Defence Industrial Base	
Commercial Facilities	
Critical Manufacturing	
Government Facilities	

Source: Angelini M., et al., 2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness, Research Center of Cyber Intelligence and Information Security "Sapienza" Università di Roma, December 2013

From table 1.2, it is possible to look and have notice of direct correspondences between US and EU critical sectors, such as *e.g.* financial services and energy sectors. This similarity is due mainly because of the strong reliance of both economies on these areas, essential for the flourishing of social well-being.

However, the two economic powers present many differences due to a different approach. Even if European Directive 144/2008 is a first step-by-step approach to identify European Critical Infrastructures, single state members define individually their own infrastructures, that put a more comprehensive protection on more areas, as it will be shown later in this chapter. US gives a more detailed list in which includes many more sectors government pays

attention to, like heritage, preservation, emergency services, government activities. A first global difference is given by government focus on agriculture, which is the base for a safe and satisfied society; therefore it must be protected by possible attacks that could cause domino negative effects on other aspects of society.

OECD defines critical infrastructure by trying to give a uniform framework for OECD members. It starts by defining what "critical" denotes, it indicates those infrastructures that provide crucial backup for all the functions that compose everyday life and business; a disruption or destruction of the infrastructure can result in catastrophic and deep damages both in physical and cyber layers. While, infrastructure, according to OECD, is referred to physical aspect of infrastructures, including in this definition also intangibles assets, like software, services or communication networks.

Canada defines critical infrastructures in order to build an effective protective strategy, as it presents massive and geographically dispersed critical infrastructures, which can be stand-alone or interconnected and interdependent within and across the territory, owned mainly by private sector (Graham, 2011). Canadian government considers critical infrastructures as "*processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government*" (Canada Government, 2009). A possible disruption of these infrastructures could result in catastrophic loss of life, adverse and persistent economic effects and a general and significant harm to public confidence in government's protection. Canada classifies vulnerable critical infrastructure in three categories physical, cybernetic and human (Graham, 2011), in order to ensure the proper security and protection at each layer.
Physical critical infrastructures are tangible assets, like roads, pipelines and transmission lines, vital establishments, as hospitals and police stations, and physically stored information, which are all considered essential to keep society well-functioning.

Cybernetic critical infrastructures include all the technology, as software, data and networks used in critical infrastructures, and all electronic information stored within these systems and that control and monitor remote management.
Canada includes also human part of critical infrastructures, as persons that operate critical infrastructures have knowledge and experience essential to run these infrastructures. If these human capabilities were lost, there would be a threat to that ability to sustain and restore critical infrastructures. Moreover, this human part can be also a real threat to critical infrastructures as potential of accessibility to physical layers and as robustness "*of management and culture to be alert to threats and build in resilience*" (Graham, 2011).
So, critical infrastructures, according to Canada, comprise series of systems essential to well-being of Canadians, treading general definition made by OECD; criticality is defined as serious impact on health, safety and security and economy of Canadians. So forth, government, in line with its definition, lists out ten Critical sectors : Energy and utilities, such as power, natural gas, oil supply chain; Finance, including banking, investments, in particular the integrity of these systems; Food, focusing on its safety during production, sales and distribution; Transportation; Government, like services and public facilities and protected sites; Information and Communication technology; Health, as hospitals, health-care and blood supply; Water; Safety, which means emergency services, security from hazardous substances, explosives and nuclear waste; Manufacturing, so chemical and strategic manufacturing.

Germany is known to be a leading industrial and technology-oriented nation. Its definition of critical infrastructures is projecting OECD definition as critical infrastructures are defined as "*organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences"* (Federal Ministry of Interior, 2009). In this setting, "critical" takes on the definition of major importance to the functioning of society, referring to significant disruptions to public order that can have dramatic consequences. A major spot is put on criticality, meant as the measure of the importance of an infrastructure relative to the impact it would have if it is

disrupted or failing on the security of providing important goods or services. German government studies the grade and the nature of criticality that can be systemic or symbolic. A systemic criticality is referred to infrastructures that have relevant interdependencies within the overall system. Electricity and Telecommunication infrastructures are a good example to see the strong interdependency thanks to their size and density of networks, and to be considered of particular relevance as a failure can lead to serious disruptions in a domino effect toward life and other critical infrastructures.

An infrastructure is considered to be of symbolic criticality if, regarding to its cultural significance that create a sense of identity and community, its loss creates emotional and psychological derangement of nation.

According to technical, structural and functional specifics, critical infrastructures can be divided into two terms: vital technical basic infrastructure and vital socio-economic services infrastructure (Federal Ministry of Interior, 2009), as shown in table 1.3.

Table 1.3: Germany's technical and socio-economic critical infrastructures

Technical basic infrastructure	**Socio-economic services infrastructure**
Power supply	Public health; food
Information and communications Technology	Emergency and rescue services; disaster control and management
Transportation	Government; public administration; law enforcement agencies
Water supply and sewage disposal	Finance; insurance business
	Media; cultural heritage items

Source: National Strategy for Critical Infrastructure Protection, CIP Strategy, Federal Republic of Germany - Federal Ministry of the Interior, 2009

UK is another country keen on protecting critical infrastructures, starting from defining what these infrastructures are. They are defined as "*facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends*" (UK Cabinet Office, 2010). From this, UK lists nine critical: Energy, Transport, Water,

Communications, Food, Health Care, Emergency Services, Financial Services and Government.

As another country of OECD, Australia defines critical infrastructures as "*physical facilities , supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security*" (Australian Government, 2010). It relies mostly on "significant" term, which indicates an event that puts risks on public safety and confidence, that can threatens economic security and that harms Australia's competitiveness or governmental functions. Critical infrastructures are characterized by strong interdependencies, also according to Australian government, like the communications infrastructure is dependent on energy supply. Australia means critical nine areas of criticality that reminds of Germany approach to critical infrastructures, like banking and finance, transport, energy, water, health, food supply and communications, key government services, manufacturing and supply chains.

Table 1.4: Summary of Critical Infrastructure definitions in OECD countries

Australia	"Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security."
Canada	"Canada's critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada."
Germany	"Critical infrastructures are organisations and facilities of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences."
United Kingdom	"The [Critical National Infrastructure] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: 1) cause large-scale loss of life; 2) have a serious impact on the national economy; 3) have other grave social consequences for the community; or 4) be of immediate concern to the national government."
United States	The general definition of critical infrastructure in the overall US critical infrastructure plan is: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." For investment policy purposes, this definition is narrower: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security."

Source: Australia: "What is critical infrastructure?" Australian National Security (www.ag.gov.au/agd). Canada: About Critical Infrastructure, Public Safety Canada (www.ps-sp.gc.ca); Netherlands: Report on Critical Infrastructure protection; Ministry of the Interior 16/9/05; UK: Counter-terrorism strategy (www.security.homeoffice.gov.uk); United States: Department of Homeland "Security Sector Specific Plans" (www.dhs.gov); Commission of the European Communities Green paper on a European Programmes for Critical Infrastructure Protection COM (2005)576

1.1.2 ACTUAL SITUATION OF CRITICAL INFRASTRUCTURES

Critical infrastructures, like financial and banking systems, electric grid and communication systems, are the lifeblood and backbone of world society, economics and politics. Their existence is woven into society's habits, therefore they are under the spotlight of governments and policy attention. It is essential that critical infrastructures are robust, reliable and resilient, able to face possible risks, coming from nature or human error or attack. Several new technology-based infrastructures have been created over the last century and half (Goodman *et al.*, 2003), their development and intensive usage characterizes modern society and its vulnerabilities.

The structure, which critical infrastructures work on, is based on the technology of control centres and on the human capabilities of operators. Critical infrastructures' control centres are made able to collect large amount of data and they can elaborate and transform them in information that provide "a *synoptic view of the ongoing situation*" (Gheorghe *et al*., 2007). Then, human operator can undertake measurable decisions in response of the situation presented by collected information.

This process is theoretically functioning but it does not take into account interoperability complexities that induce human operators' capabilities to be more sector-specific. Complexities come from the subtle interactions between critical infrastructures and subsystems, which are hidden and not well understood by the experts and operators. The paradox underlined by Gheorghe *et al.* (2007) is that this hidden interaction is the common thread of coping with these systems and the main cause of cascading and domino effect failures.

What makes these complexities more complex to handle is that the majority of critical infrastructures have not been designed to be part of an integrated system, but they have been just evolved gradually over time to accomplish required tasks. New nodes are added to already existing networks through other selected nodes, this happens to electricity and natural gas infrastructures as well as internet infrastructure. The associative or preferential network system presents the advantage to build a robust network, able to resist to multiple failures of random nodes. However, this configuration exposes the entire

system to targeted attacks and failure that might induce risks and damages to other interconnected systems (Gheorghe *et al*., 2007).
Critical infrastructures are structured and divided into three levels, each of them considered as nested subsystems, independently analysed and protected. The levels are hierarchically overlying and start from micro-level, which represent physical components, meso-level, *i.e.* infrastructure network represented at system level, and macro-level, which outlines the zone or area which is dependent on the service provided.
Consecutive spread is assumed by Gheorghe *et al*. (2007) coming from bottom to top level, denying possible downstream consequences and outages.

The framework changed since factors have transformed the innate nature of infrastructures, influencing design, development and deployment of these infrastructures. First of all, liberalization of markets, mainly regarding electric power and telecommunications, opened the networks to more players, arising problems of attribution about risks and costs regarding security and maintenance. The segmentation provoked by liberalizing markets puts problem on the effectiveness of risk-management solutions that are undertaken by single players that tend to not have an overall understanding of risks spread over the systems, even if recognised as basic public services and therefore under governmental regulation. Moreover, the inter-working among infrastructures, which is required in order to complete functioning, generates strong interdependencies between systems, fostering the spread of failures to one system to another. This worsens the comprehensibility of systems and their interactions with environment, consequently potential threats are misunderstood or wrongly addressed as it is difficult or nearly impossible to understand networked environment, since it is important to understand the defined interactions among systems.
A consequence of interdependencies is the increase in cross-border interconnections, essential "*to share capacity in case of major malfunctions*" (Gheorghe *et al.*, 2007), which creates mutual dependency on the functioning of numerous infrastructures, providing services and at the same time being a possible source of risks and failures. A door to malicious attacks is left open by advancement in technology connecting systems through open public networks,

accessible so by both legitimate users and hackers. This vulnerability jeopardizes reliability of systems and risk governance, which now has to deal with much more risk factors and to address effective and efficient solutions integrated in the management process.

Since here, a bunch of terms are outstanding and essential to understand the importance of sane critical infrastructure.

The first term expresses a new approach to risk management, risk governance. It focuses on systematic risks in systems with high degree of complexity, uncertainty and ambiguity, and that have repercussions on finance, economics and society. Risk governance requires stakeholders involvement, thus national authorities, international organisations and businesses and end users. It recognizes stakeholders' individual interests and points of view, and it always keeps in mind the overall objectives to be pursued. It has been modelled an IRGC (*i.e.* International Risk Governance Council) risk governance (Renn, 2005) which fosters an integrated and analytic framework for risk management providing guidelines for developing and understanding strategies able to cope with risks at a broader level; this model puts together various aspects, integrating scientific, economic, social and cultural sides.

These aspects must be taken into account during the decision-making process, constructing a multi-criteria problem around the diversity of objectives and actors implied. What is new in this model is the focus given to socio-cultural dimension of risks, which influences actors' reactions to risks, and it is described by the understanding and the response to risk governance process by social actors, like public, *i.e.* end users and business, and governments. It is essential for effective risk governance that actors cooperate to cope and handle risks that go beyond the boundaries of their own risk management strategies. These risks can involve numerous actors or that exceed the control of one actor.

The template suggested by International Risk Governance Council, based in Geneva since 2003, divides the process in sub sequential 4 steps plus communication (Perks *et al*., 2009). It starts from Pre-assessment step, which involves acquiring a broad picture and understanding of risks. In order to provide a well-structured definition of the problem, it is essential early warning

and framing of risks, taking into account also different framings of other stakeholders, by gathering as many information about their responsibilities as it can. Then, at Appraisal stage, it combines (Perks *et al*., 2009) scientific risk assessment, *i.e.* assessment of hazard and consequent probability to happen, with a systematic concern assessment of public concerns and perceptions, in order to provide the basic knowledge for further decisions. Characterisation and evaluation stage assesses the acceptability of risks, using scientific data and social values about risks, evaluating risks as acceptable, tolerable and so that it can be mitigated, or unacceptable. It can be useful to construct a risk tolerability matrix, with potentiality of risk impact and system vulnerability, in order to clearly understand the rate of risks. Then, Management identifies the actors, actions and timing to put in place. An effective risk management includes the design, the implementation and the monitoring of the effectiveness of undertaken activities. This makes the strategy adaptable and evolving along with increasing and differentiated risks. Along these stages, Communication goes parallel, as it accompanies each stage and increases the cooperation between actors and fosters the process effectiveness and fast response to risks.

Then, there are three terms used for describing a sane critical infrastructure that are related also to risk management and risk governance, reliability, robustness and resilience; while related, these three qualities covers the spectrum of steadily performing systems.

First, there is reliability, which is the ability of a system or part of it to function under certain conditions and for a specified period of time; it can be defined also as the frequency of failures. Reliability analysis, generally, deals with component or sub-system level and expresses the mean time to failure or to repair (Conrad *et al*., 2006), in order to project estimation of equipment availability for restoration and mitigation of failures. It means dependable and persistent, it is not prone to casual breakdowns not even due to component or parts failures.

Robustness means "*having or exhibiting strength or vigorous health*" (Little, 2002), it points strength and durability, and it is a quality and a capability of physical aspects of infrastructure; therefore, as Larson *et al*. (2005) precise, a

residential electrical distribution network is more robust when it is underground than an above ground system.

Finally, there is resilience which measures the capacity of a system potentially exposed to hazards to resist or to change in order to maintain an acceptable level of functioning (Emergency Management Framework for Canada, 2011); the Canadian framework leaves to subjectivity the definition of acceptability and criticality levels. According to Larson *et al.* (2005), resilience describes a flexible and elastic system, which is able to bend under stress without reaching a break point, and, in the meanwhile, minimizes risks of cascading failures due to equipment breakdown that could lead to major blackouts; it includes the ability to recover rapidly from disruptions, or deliberate attacks, accidents or natural threats (PPD-21, 2013). According to *National guidelines for protecting critical infrastructure from terrorism of Australia* (2011), resilience includes activities that range from prevention, preparedness, response and recovery to hazards, which include natural disasters, pandemics, negligence, criminal activity and terrorism.

An infrastructure is resilient when it is also robust, agile and adaptable, and when mitigation, response and recovery actions and strategies are well implemented and functioning. In order to achieve resilience, it is necessary to collect accurate information about risks, so it is indispensable to put in place an efficient and effective risk governance strategy.

Critical infrastructures, like energy, water and telecommunications, are vital and ubiquitous, therefore their lack of capacity or even their destruction affects not only security and social issues of one nation, but it has devastating cascade effects across borders nations. These connections are the base of a complex web, and are the reason of shock transmissions across borders and across numerous infrastructures. Nowadays, it is practically impossible to consider and analyze a single-standing infrastructure isolated from environment or other infrastructures. It is possible to identify various typologies of interdependencies in order to analyze and forecast risks and possible path of propagation (Rinaldi *et al*., 2001).

When infrastructures are dependent on material output of others, there is a physical interdependency, which arises from physical linkages among inputs

and outputs. At this interdependency, a possible failure takes place when timing of exiting outputs of one infrastructure and entering of inputs of another does not coincide, creating buzz and inefficiency.

A new interdependency is appearing and it is cyber interdependency, which takes place when an infrastructure is dependent on information transmitted through communications system. It is evident in the massive and increasing use and reliability of computerized control systems, from SCADA systems which is in charge to control electric power grids to other systems that manage the flow of goods over railways.

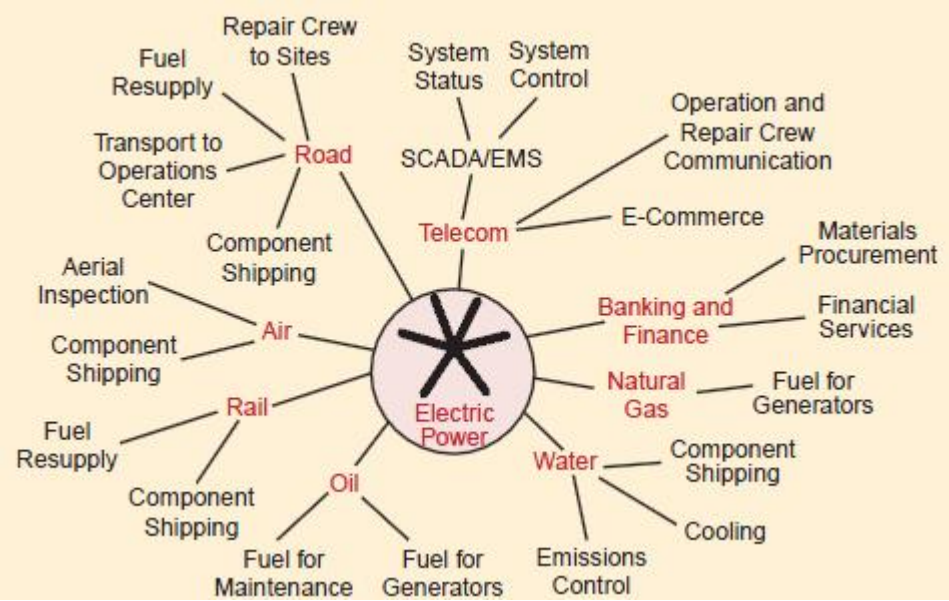
Geographic interdependency describes geographic relation among infrastructures that are in close spatial proximity, and it is particularly important for security issues, especially when natural or terroristic damages can easily spread over other proximal infrastructures, creating correlated and simultaneous disturbances in the overall system environment.

Two infrastructures are logically interdependent when they depends on the state of others via mechanisms that are not physical, cyber or geographical. But, it is related through a control scheme linking agents in the infrastructures. Here, it is clearly visible the strong human factor and his predominant role in decision making affecting also critical infrastructures functioning.

A great importance among critical infrastructures has energy sector, which includes power generation, transmission and distribution. Indeed, electric power has conquered a bigger and more important responsibility, therefore it gains a principal role in society and economics, as the leader toward progress before in now-developed countries and now in the developing ones. Electricity is considered by societies as an inherent component (Gheorghe *et al.,* 2007), which is indispensable for achieving and maintaining the expected or attested level of life quality. Electricity is considered as a common good, central to the security and welfare of almost a half-billion people and essential to the stability and economic developments of more than 30 countries (Perks *et al.*, 2009). The most populated regions are Germany, the UK, France and Italy. It is interesting to notice that it is foreseen an increasing final demand of electricity, from 8% registered in 2005 to 28% expected in 2030; this fast pace of growth will require an additional generation capacities, that could be filled by renewable

resources. Natural gas consumption is expected to increase with respect to 2005 level, from 445 Mtoe (i.e. million tons of oil equivalents) to 516 Mtoe in 2030. The increasing demand reflects the growing dependence on imports that EU members have. According to Perks *et al.* (2009), the totality of EU members depend to some extent on imports from other states in order to be successful to meet energy demand; this dependency is expected to reach 70% of internal demand in the long run. Electric power infrastructure can be considered as the pillar of infrastructures, characterized by strong and deep interdependencies with all other essential systems.

Figure 1.1: Electric power infrastructure's interdependencies



Source: Rinaldi S.M., Peerenboom J.P., Kelly T.K., Identifying, Understanding and analysing critical infrastructure interdependencies, IEEE Control Systems Magazine, Dec.2001

As shown in Figure 1.1, it is evident that electric power infrastructure is interdependent with other critical infrastructures, and it depicts clearly how a malfunction could spread over other systems, creating cascading failures. According to Rinaldi *et al.* (2001), electric power system is standing upon other critical infrastructures for its own well-functioning, so under normal operating conditions it needs natural gas and oil in order to power generators, moreover roads, rail transportation and pipelines are required for supplying the generators; also air transportation is needed in the electric power system as it is for aerial inspection of transmission lines; water is vital for cooling and

emissions control; also banking and finance infrastructures influences electric power, since they are in charge to set fuels price; monitoring and control systems, like SCADA, and energy management systems are in control of telecommunication infrastructures.

These interdependencies make electric power essential to society, as it affects end users of any infrastructure, socio-economic activities, like banks and government and at macro-level other infrastructures laid on electricity, furthermore, if extreme situation happens, security would be flawed (Thissen, Herder, 2003).

Electrical system is under a growing stress caused by the increasing demand, the impact of deregulation on investments and, consequentially, the lack of coordinated strategic planning; all these factors undermine the security of the actual system and the robust expansion (Larson *et al*., 2005).

Researchers have particular interest on the European electric case study, as it presents a difficult network spread over a continent but essentially divided into more regions with different capacity and legislation; EU is focus on keeping a sustainable, competitive and secure access to energy sources (Green Paper, 2006).

Blackouts and failures happened in last years in Europe have brought to light inefficiency that must be addressed in order to foster electrical network. In *Critical infrastructures: the need for international risk governance* (Gheorghe *et al*., 2007), it highlights a situation of inadequacy, as system is exposed to vulnerabilities because of heavy workloads and limited reserve generation capacities. It results from the study that power systems cannot cope with a simultaneous outage of critical components. Another aggravating factor is the shortness of time to response adequately to potential failures and short-term emergency needs. Currently, operators depend on measured information in order to monitor the present status and to take control actions on, therefore, in order to take conscious and effective actions in emergency or fast-response situations, powers system control must provide reliable, accurate and complete data for monitoring and controlling power system in real time. Moreover, electricity market liberalisation leads to increasing cross-border trades, replacing a centralised control characterized by national monopolies with the

complex decentralised market structure, whose many players have control of a part of technically and highly integrated electrical system.

The evolution of electrical infrastructure in Europe is following a two-tier path, a legislative one and a physical one. In the last decade, EU has dealing with this infrastructure policy, developing a comprehensive energy supply by unbundling monopolies and opening supply chain to other players (European Commission, 2003). This liberalisation represents the world's most extensive cross-jurisdiction reform acting in electricity sector, integrating distinct and numerous state-level or national electricity markets (Jamasb, Pollitt, 2005); it has deeply changed the dynamics of players and consumers' impact. In fact, energy players start facing more competition, that has a positive impact on consumers as prices go down following open market rules.

However, economic effects produced by the opening of market barriers have not accompanied changes in physical systems. Physical improvements need medium-term investments, and, even if the system proved to be reliable, new threats, that can be internal if due to increasing technical or market complexities, or external because of terrorism threats, may be faced in the short run that need to be handle. The first issue to be addressed by EU is the growing ageing energy infrastructures that require massive investments, the replacement would present, however, some side effects, in fact older equipment employs old style or basic electromechanical or stand-alone controllers which are actually less prone to cyber attacks, now there is modern digital control equipment linked to DCS, *i.e.* digital control system, and SCADA, *i.e.* supervisory control and data acquisition. SCADA, in particular, is a system which collects, displays and stores information from remotely located centres and sensors that helps controlling equipment, devices and automated functions, that constitutes energy infrastructures. This system brings advantages to business as an increased competitiveness through the ability to control multiple processes at one time, the reduced travelling costs for supervisions and the pro-active management. But, how SCADA has been adopted by more centres in the network, vulnerabilities appeared frequently as it is more subjected to malicious attacks, which may create far greater damage than keeping ageing equipment, because SCADA systems are dependent on

common software, common operating systems, and the Internet. SCADA is sensitive to four major threats (Perks *et al*., 2009) that are malware, insider attack from employees, hackers and cyber terrorists, threats that will be addressed later in this dissertation. Security, in this way, becomes the first issue that policymakers have to address, as a multiple attack could result in several disruptions at different sites, or failures on transmission lines that could cause instability at SCADA system level.

According to Perks *et al.* (2009), Europe needs to be fast in collecting and addressing investments suitable to meet the expected growing energy demand and to replace ageing infrastructures that amount around one trillion euro spread over the next 20 years.

Numerous national European electricity infrastructures form an integrated network called European Critical Electricity Infrastructure (ECEI). This strategy to unify and homogenise fractured systems expresses the internationalisation trend, at policy, economic and technical level. First of all, Europe faces jurisdiction fragmentation, visible through the different speeds that liberalisation had and the diverse implemented models, taken without considering global consequences and repercussions. Legislatively, the trend of liberalisation and internationalisation is difficult to harmonize as it must take into account local member changes in environmental standards, taxes and subsidies, which all of them threat the reliability of provided electricity services (Gheorghe *et al.*, 2007). Moreover, taking a stakeholder point of view, reaching a Pareto Optimum solution is even more difficult as many actors and many countries with different interests and requests take part to the overall infrastructure.

At technical level, there is need of cooperation among system operators, which can ensure a functioning integrated electrical system.

Integration is more difficult at economic level, as large differences persist in different markets. Therefore, European members need to create a secure international electricity market, where economic conditions, like tariffs and network access rules, could be in synergy.

What makes interesting electric infrastructure is the growing use of renewable energies, which causes the so-called evolutionary unsuitability (Gheorghe *et*

al., 2007). Electricity system are increasingly used in ways different from which it was initially designed, worsening network functionalities as it has to resist rapid operational changes triggered by the use of renewables. First of all, a source of stress for electricity system come from wind power, as "*the electric output of wind parks lead to fast and significant changes in the way the electricity network is used*" (Gheorghe *et al.*, 2007), that could lead to significant stability problems.

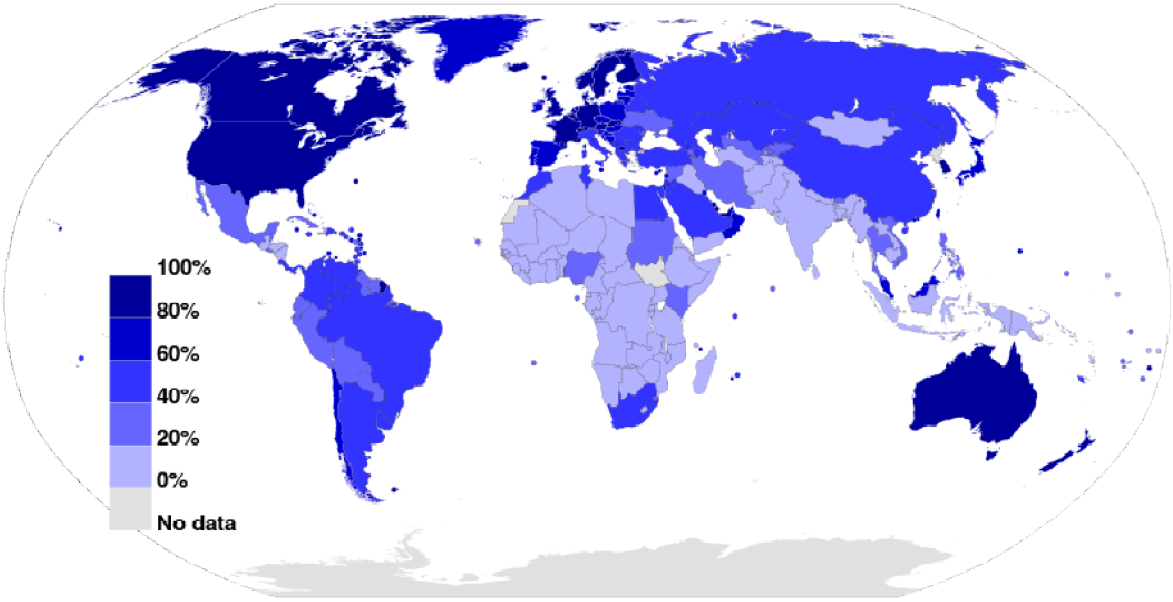
Then, stress come also from the canalization and transmission of renewable energy, since sources are geographically bound while the consumption can be required in another region. Therefore transmission and international interconnectors are essential for this kind of new resources. And so, also security and control systems must be well-functioning and operative in order to be efficient and effective also under stress or under attack. According to Gheorghe *et al*. (2007), in order to shut down a large part of European electrical system, it would be required a sophisticated and well-coordinated attack.

Along with electricity, telecommunications infrastructure has become the key for functioning economic and social systems, in fact, it is essential in the exchange of services and goods between countries and businesses and it represents a channel "*in changing economic interrelationships through rapid technological change and the proliferation of a range of new services*" (Sarrocco, Ypsilanti, 2008). Internet is driving as a leader the central role of this infrastructure in socio-economic life, and also in every-day life. Thanks to a wider access to higher speeds, both to residential users and to business, the role of telecommunications increased along with the expansion of the offered services and the ease of accessing them for a broader pool of users. However, the actual situation can be improved by ensuring universal, or close to, geographical coverage, and, for doing this, markets must be effectively competitive, lowering barriers to entry and providing reliable services.

In *Convergence and Next-Generation Networks* (2008), OECD enlists the power of Telco markets, as it has surpassed 1 trillion USD in revenues in OECD area, and it is expected a growth of 3% per year, in real terms, thanks to its increasing role in nations GDP that exceeds the decreasing prices that sector

is facing. Investments, also, has demonstrated to be increased in 2003-2005 period by 24%, driven essentially by a growing demand for broadband and data access.

Figure 1.2 : Internet users per 100 habitants 2006-2013



Source: International Telecommunications Union (Geneva), [accessed 17th November, 2013], http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2012/ITU_Key_2006-2013_ICT_data.xls

In Figure 1.2, it is possible to observe the wide spread of broadband subscriptions, that had an increase by 60% per annum over the last 5 years in OECD countries. Of course, the rate of subscription and Internet penetration differs from country to country, with US and Canada, Europe and Australia showing the higher rate in Internet users. Other differences are in the rate of subscriptions for different multimedia tools, indeed, for broadband subscriptions it has been reached 19 subscribers per 100 inhabitants, a number that, in comparison to 80 mobile subscribers or 43 telecommunication channels, represent a scarce figure but, however a starting point for a wider, more easily and comfortable access to the Internet, since it is the fastest growth in Telco penetration rates.

Technological innovation and development is the driving force in this market, as costs are reduced, while the capability of networks is increased and improved in order to support new and more sophisticate services and applications provided. The major change that would bring benefit to society is

the change toward a new technology, based on packet-based network that use Internet Protocol, and that is called Next-Generation network (NGN). NGN underlies the shift to higher network speed thanks to passage to IP-network; this can ensure a greater tolerability of different services on a single network and offers access to different service providers and allow mobility and consistent and ubiquitous provision of services. The International Telecommunication Union (2004) describes NGN as "*packet-based network able to provide services including telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service related functions are independent from underlying transport-related technologies*."

This is the response to the ongoing development of a universal access to Internet, but that require substantial investments that countries must face in order to replace existing technologies with fiber technology. Even if fiber cables are considered to be resilient and reliable, the large pool of alternatives and options gives an advantage to incumbent operators and new entrants. In fact, NGN is compatible also with existing technologies, which would not require significant investments, as copper networks, that have to be upgraded to DSL, coaxial cable networks, power-line communications, high-speed wireless systems and also hybrid technologies.

NGN can be the answer to economic, technological and social problems that rose in last years, because of fossilised strategies adopted by telecommunications operators. Economic drivers for the adoption of NGN is the continuous erosion of fixed-line voice call revenues, caused also by saturation of fixed and mobile telephone services, a growing competitive pressure made by new entrants in high margin markets and from vertically integrated operators. NGN can also expand business into new market segments, meanwhile it is possible to retain and expand users' base and to lower customer churn, taking advantage of ladder of investment, so absorbing higher revenues from densely populated areas, in order to finance a progressive expansion.

NGN would be well accepted also because it can make possible the turnover of obsolescent networks, which are the source of plus costs and complexities. NGN can ensure lower capital and operational costs, increased centralisation of

routing, switching and transmission, moreover it will guarantee lower costs of transmission with respect to optical networks. Moreover, it is possible to provide cheaper VoIP services and also a wider range of services over NGN, allowing services bundling (Sarrocco, Ypsilanti, 2008).

Society is, anyway, asking for this revolution, as it require more and more innovative services that request high bandwidth, like VoIP and HD TV, users ask for targeted and personalised contents, like on demand services, mobility and multimedia services, therefore, it is also required interactivity, which can trigger the interest of users in creating new contents. The segmented markets ask for flexible forms of communications, as instant messaging and video conferencing, and integrated services, which are useful for multinational firms because they can embody flexibility and security for their business.

However, NGN can represent a possibility for improving services provided over the Internet, but it can be also seen as a constraint of Internet into telecommunication boundaries, with more and new control layers, that can discriminate provided contents and make them turn in profits, by squeezing users willingness to pay.

For sure, NGN will be differentiated from public Internet which uses the best effort approach, then it is subjective to traffic loading and network status of congestion. Instead, NGN is enhanced with Multi Protocol Label Switching, which ensures a higher degree of Quality of Service, experienced by users, traffic prioritisation, and other techniques that optimise the efficiency level of network.

Telecommunication system is the sum of three structures, which ensure its vitality and open the road to economic agreements in developing countries. Active infrastructures comprehends spectrum, switches and antenna, passive infrastructures are towers, BTS shelters, power supply, generators and so on. And there is backhaul, which are "*core network elements such as switching centers, GPRS service nodes, transmission equipment and all links connecting elements of the core network"* (kpmg, 2011), and it is concerned with transporting traffic from one site to another.

As economic strategy, operators tend to share passive structures, which bring a decreasing in infrastructures spending, to a rationalization of operational costs and a focus on innovation of services.

Telecommunication infrastructure has a similar importance of electricity, and it is an essential part for emergency services infrastructure (Conrad *et al*., 2006). Partial or complete failure of this infrastructure could lead to chaos and discomfort, as society dependency on communications tools is far increasing; moreover the failure can lead to property damages and, worse, to loss of life, by just causing delays and errors in emergency responses.

The fragility of telecommunications infrastructures is a historical fact, since telecommunications tools have been the first targets to be destroyed in order to destabilize enemy, because telecommunications system have not had high degree of redundancy (Townsend, Moss, 2005), therefore the failure of single segment could disconnect a larger area. Technology developed new telecommunications networks by designing them more physically resilient to attacks or natural disasters, the Internet was created. However, even this new form of telecommunications is not completely immune to vulnerabilities. The weak nodes are key interconnection facilities, called Telco hotels, that are located in major cities and linked to small business and households through old copper wire, but vulnerable is also wireless links, as they are subjected to physical destruction, such as weather and debris. Moreover, new technologies like Wi-Fi cannot be considered too much reliable in emergency situations, because it can cover a small part of geographic area.

The stress caused by urban disasters is overloaded on telecommunications networks, and it is greater if the geography of destruction includes both old and new facilities of telecommunications (Townsend, Moss, 2005), therefore the physical destruction of system components can lead to the disruptions of telecommunications.

Telco failures come from disruptions of complementary supporting facilities, as telecommunications infrastructures have significant interdependencies with power supply, water infrastructure, which is essential for cooling systems, as demonstrated in Northridge earthquake in 1994, and also fuel supply, which powers electrical generators. It is funny to notice that amateur radio works

even under disaster stress, and it has demonstrated more resilient than other sophisticate telecommunications tools, in fact during disasters, radio teams work in conjunction with governments and emergency services in order to restore rapidly critical basic infrastructures (Townsend, Moss, 2005).
Overloading is frequent during crises and it is another cause of failure of telecommunications, since emergency services need to coordinate activities and to communicate information about people and status of damages. But, telecommunications systems are also put under stress because of panic reactions that involved persons experience during disasters. Townsend and Moss (2005) say that Northridge earthquake in 1994 had registered the highest peak in phone calls, it is remembered as "*single largest telecommunications event in human history*" (Townsend, Moss, 2005).

In Europe, the focus has been put on Next Generation Networks, based on fiber technology, and, according to Lancaster (2013), the completion of resettlement from copper networks to NGN architecture is due by 2020. This transformation is encouraged by EU programme which establishes to provide higher broadband to citizens up to 50Mb/s by 2020. This gives stimuli and momentum for regional infrastrucutre upgrades, accompained by spectrum auctions for several bands, revenues that finance EU targets. In fact, as the crisis stroke European members, public investments arrested and now it is all on private sector back to foster Telco infrastructures development.
Regulatory organs have to be carefull to maintain a sane competition and ensure investments would not dissolve. Reducing carbon emissions is on European agenda, and it is possible by requiring intelligent electricity grids based on upgraded telecommunications networks, creating trans-sector synergies and benefits

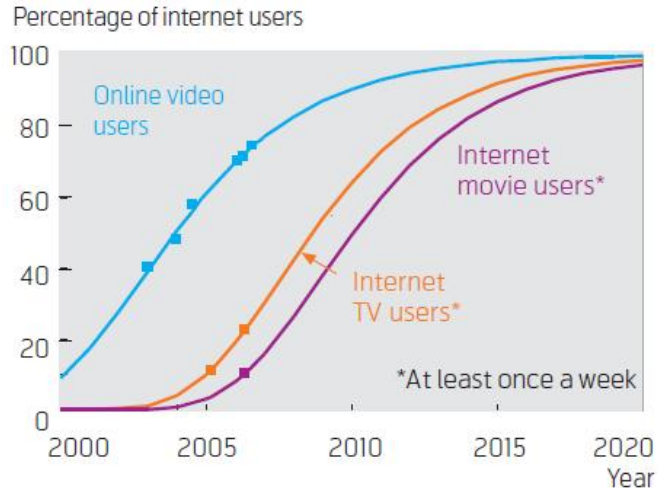
In US, competition among providers is stricter as equal services are provided by more operators with different QoS and prices, so along with mobile and fixed telephones there is VoIP, there is broadcast and IPTV, but also a new branch of digital economy, as smart energy grids, e-health, e-government and e-education (Baker, 2010).

Cable companies, using new technologies, make revenues over "traditional" landline companies who lose, as cable VoIP subscribers are expected to continue to grow as well as cable modem subscribers. Mobile market is opening access to 4G platforms that sensitively increase the possible scope of mobile broadband usage.

A notable trend is that mobile phone usage is directed more to data elaboration and receiving, with a growing number of mobile phone users with respect to fixed phone, substituted by wireless broadband. In the future, mobile wireless is expected to substitute significantly wire line connections, since wireless systems, as WiMax and 4G, are going to have sufficient capacity to provide services and applications to a growing number of users. As more Wi-Fi tools are demanded by consumers, in US it is expected a new generation of municipal Wi-Fi hotspots.

The increased demand for capacity and quality is driven by video services, shown in Figure 1.3, distinguished in online video, the most famous example is YouTube, whose services are linked to bandwidth and other factors of transmission; IPTV, television services in competition with cable channels, it uses a dedicated broadband link to the customer (Vanston, Hodges, 2009); Internet TV, like streaming and downloading from open Internet, it is different from IPTV since the carrier provides just the broadband channel and not the programming.

Figure 1.3: US online video users and Internet TV users



Source : Data source: OL Video: eMarketer, Nov 2006 & Comscore; OL TV: Online Publishers Assn in Vanston L.K., Hodges R.L., Forecasts for the US Telecommunications Network, Telenor ASA, 2009

Therefore, US is requiring to Telcom operators to install and upgrade infrastructure to Very High Speed (VHS) broadband, that ensure QoS and speed for those services which are time dependent, like e-health and video conferencing. VHS requires fibre-based loop architectures (Vanston, Hodges, 2009), and it is expected the final conversion to VHS in 2015, when wire line broadband subscribers will move to this new efficient system.

1.2 ECONOMIC AND POLITICAL CONSIDERATIONS

Critical infrastructures are systems that live in symbiosis with the environment that sourround them, demonstrated by strong and deep interdependencies (Rinaldi *et al*., 2001). The global environment in which critical infrastructures are plunged is defined as infrastructure environment, and it frames the cooperation needed between owners and operators in order to establish objectives and to model strategies and operations (Rinaldi *et al*., 2001). This environment is very sensitive to influences radiated by each infrastructure, which, at their turn, are influenced by the overall changes in the external environment.

Rinaldi (2001) discovered forces that can shape the environment and shape its characteristics. There are economic and business opportunities and concerns, which are driven by new opportunities possible thanks to technological innovation. However, this can lead to constraints on operational characteristics, decisions and infrastructure architecture and topology (Huffaker *et al.,* 2012).

Regulation, or deregulation, can change significantly the rules of competition, which manipulate profitability, image and business concerns. Therefore, public policy is another environmental dimension, which can affect infrastructures analysis and security. In fact, thanks to legal and regulatory plans, the security and well-functioning of these infrastructures is guaranteed by setting legislative borders and appointing boards that can control and rule over infrastructure. The decisions taken by these legislative organs have direct effect on infrastructure economy and policy*, e.g.* FCC (*i.e. Federal Communication Council*).

By deciding to not regulate Internet it has been the driver of a booming growth in US information technologies. Moreover, governments have a key role in influencing and directing investments in creating or improving infrastructures, particularly on those technologies that are risky and with no monetary return that private sector would not be interested in.

Also social and political issues can transform infrastructure environment, in fact, politics can easily create the perception of need of any laws or regulation that directly influence infrastructure behaviours and society can effortlessly require new approaches to economy and security, therefore requiring new

approach also about critical infrastructure strategies. In a globalised world, these forces are international, just as infrastructures. Macroeconomic changes, due to international agreements like OPEC or because of political instability in countries with high discretional power, influence in particular those infrastructures that tend to be more international, like telecommunications, banking and finance and oil and natural gas.

All these concerns and issues are important variables in the infrastructure environment, and must be considered in the comprehension of interdependencies and environment. Policy should address proper strategies that would comprehend structural, organizational and financial issues in order to improve critical infrastructures (Hammerli, Renda, 2010). It should be balanced strategies pointed for prevention and strategies aiming at emphasizing resilience and auto-adaptive characteristics. Strategies have to focus on security and prevention actions, to promote a constructive dialogue among parties, and to give incentives for private investments.

In Eckert (2005), it is outlined the importance of cooperation among private and public sectors, since they are important actors in security concerns. And, with 85% of US key infrastructures that are privately owned or managed, it is essential the coordination of actions on the part of government and private actors in order to establish an integrated homeland security.

Security and resilience are addressed by owners and operators that support risk management planning and bear investments, that are calculated balancing a trade off among risk and consequences. Risk is levelled upon information retrieved from federal government about risk environment. The consequences are measured considering economically justifiable and competitively sustainable actions (U.S. Department of Homeland Security, 2013). For these measures, it is important the cooperative dimension by participating in collective efforts in order to improve security and resilience by providing timely warnings and appointing specific responsibilities.

The investment made in cooperation mood have benefited the entire US nation as security and resilience have made been essential and central in strategies. Risk mitigation plans are first step for reaching a better protection of networks,

it implies employing cyber security, sharing information about risks and threats.

Collaboration among private firms and governments can be either statutory or voluntary, depending from sectors regulation. Voluntary collaboration is the primary tool for serious collective actions toward critical infrastructures security and resilience; in fact many sectors have established a stable and significant partnership in order to widen the range of members and skills needed to reach the prospected objectives. These relationships help, moreover, governments as the information retrieved and collected give a deeper understanding of risks and actions taken to be prepared, in this way decision making processes are more informed and assessed.

From economic perspectives, in order to put order in accounting and economic concerns about critical infrastructure, the Centre for the Protection of National Infrastructure (*CPNI*) (ICE, 2009) has started to identify the most vital critical infrastructures in order to take actions in protecting them by creating a national asset database. Mapping and understanding the real conditions of critical infrastructures is the objective of CPNI database, the first step toward a more integrated management of these systems.

From the database it should be easier improving accounting system finally able to recognise precisely costs and the current value of infrastructures. For doing this, government has to carries out cost benefit analysis of infrastructures, including building and maintenance costs, and comparing them to the cost to society, environment and economics if they were to fail.

In 2008 it passed the Planning Act that would provide a more efficient planning system for significant critical infrastructures, such as railways, ports, roads, airports, water and waste. It establishes an independent Infrastructure Planning Commission to correctly determine detailed and technical contribution of individual applications. However, the main focus of policymakers is not improving resilience and reserve capacity but it is more concentrated on consumers' side, so price and level of provided services, leaving these more urgent and significant aspects to the market, since regulators do not have the ability to incentivise asset owners to build reserve capacity (ICE, 2009).

In conclusion, it is possible to recognize the importance given to critical infrastructures by policymakers and economists, since these networks carry on the worldwide society. The economic and political aspects of critical infrastructures make difficult to approach them, since an improvement in either side would provoke infinite effects, which could be positive or not, in many others fields and sectors due to deep and hidden interdependencies.

The strong reliance on critical infrastructures must be protected by ensuring a sustainable partnership among private and public sectors in order to address effective improvements in defense and resiliency.

1.3 COPING WITH MALFUNTIONALITIES

Critical infrastructures play a vital role in society, as they provide most basic facilities for modern societies.

Physical parts of these networks have to undergo to alarming range of threats coming from nature, like earthquakes, extreme winds, floods, snow and ice, volcanic activity, landslides, tsunamis, and wildfires, but also threatened by terrorist acts, design faults, aging materials and inadequate maintenance. Maintenance itself is a key aspect against failure, but it is also the aspect less assessed by investors, declining constantly the resilience of systems and thus increasing the probability of severe failures.

Failure of major infrastructures could provoke catastrophic effects, indeed the failure of these significant systems, like it could be water, energy, waste and transportation, can cause environmental damages, important cost to economy and possible threats to life.

Although analysis of past catastrophic events, the improved prediction and forecasting methods and a better engineering approach to these infrastructures, important failure still occurs and the consequences of failures can range from harmless to noxious (Little, 2002).

The solutions to failures is to adequately maintain and protect critical infrastructures and to build reserve capacity, useful during emergency actions; it is essential for this purpose to include better private sectors, since they can easily and better assess systems status and address proper protection (Brömmelhörster *et al*., 2004).

1.3.1 MILESTONE CASES OF MALFUNCTIONS

It is important to protect critical infrastructures from failures that can propagate and jeopardize entire areas. Disastrous failures show a constant and subtle link between technology and human performance. Human action, or lack of it, has a critical role in managing complex infrastructure systems under stress or during crisis, and human role need to be better understood as it has a deep connection with entire life cycle of disasters (Little, 2002).

Understanding the origin of those infrastructure failures and their propagation patterns is the key to prevent catastrophic event or at least make networks more resilient. For this purpose, it is opportune to dedicate attention to past significant cases of malfunctions that occurred and to analyze mitigation and restoration plans, in order to spot vulnerabilities.

In US there were many cases of physical failures of critical infrastructures that could be attributed to a mix of natural and technical contribution. In fact, even if most of the times failures tend to happen during adverse weather situations, critical infrastructures are less robust and resilient because of human error in measurements and assumptions in technical assessment and design. Many accidents can be conducted to these causes, like collapses of bridges or construction due to mistaken design.

Because of lack of maintenance, Mianus River Bridge [2], in Connecticut, which carried Interstate 95, in 1983, fell into the river and it resulted in the loss of three lives (Little, 2002). This accident could possibly have been avoided if deeper and constant inspections had taken place, in order to assess the status of the structure properly.

The collapse of Schoharie Creek Bridge[3], which carried New York State thruway, happened in 1987 because a cut pier fell into the creek and bridge girders slipped off their supports. This provoked the falling off the roadway and caused the death of ten people. What makes this failure even more tragic is that a report about the need for replacement of missing riprap around the cut pier was presented ten years before, but foundations have never been properly inspected.

Another case caused by poor inspection and maintenance practices and a lack of redundancy in design is the crash of a bridge[4] that carried US route 51

[2] NTSB (National Transportation Safety Board), Collapse of a Suspended Span of Route 95 Highway Bridge over the Mianus River, Greenwich, Connecticut, (HAR-84/03), National Transportation Safety Board, Washington, D.C., 1984, in Little R.G., Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems, 36th Hawaii International Conference on System Sciences, 2002

[3] NTSB, Collapse of New York Thruway (I-90) Bridge, Schoharie Creek, near Amsterdam, New York, (HAR-88/02) National Transportation Safety Board, Washington, D.C., 1988 in Little R.G., Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems, 36th Hawaii International Conference on System Sciences, 2002

[4] NTSB, Collapse of the Northbound U.S. Route 51 Bridge Spans over the Hatchie River near Covington, Tennessee, (HAR-90/01), National Transportation Safety Board, Washington, D.C., 1990 in Little R.G.,

because two columns that supported three bridge spans collapsed killing eight persons.

In 1981 it happened "*the worst structural disaster in the United States*" (Levy, Salvadori, 1992), when the Skywalk at Hyatt Regency Hotel in Kansas City collapsed and killed 114 persons and injured more than 200, because of series of events that occurred damaging the structure. In fact, the sequence of events started with a wrong design that made unbuildable the Skywalk, then the design was modified in order to ease the constructability that just made weaker the construction, these changes were not noticed by structural engineers, and when deficiencies showed up during the building they were not adjusted.

These major examples show how important is the security of critical infrastructures. It must be a going-on process starting from the correct design and must continue with the maintenance and inspection controls in order to take control over the frequent intersections among technical faults and human actions.

Among critical infrastructures, telecommunications networks are crucial, since interdependencies with other basic infrastructures is basilar to share information. Any disruption is possible the cause of significant disturbances in everyday life of any entities, like households, banks, public and private businesses. Therefore, because of their importance, there are concerns to make IT infrastructure secure and reliable in order to maintain equilibrium among this living environment composed of all critical infrastructures.

Failure of this system can come from physical interruption, like malfunctions or damage of physical tools that compose the entire system, or from terrorist attacks, that most of the times come from the Internet itself. In order to construct an efficient security strategy, it must be clear the tactics and techniques and targets of possible and probable attacks. This topic will be faced more in deep in the next chapters, however here it is useful to understand the connections of information and telecommunications infrastructure with the bigger system of infrastructures.

After 9/11, protection of these infrastructures against online attack has become government priority (Anderson, Fuloria, 2009). This is commonly interpreted as preventing online felony against physical utilities, like electricity, water and transport networks, but on terrorists' list there is complex mix of political, economic and psychological targets to strike by causing mass casualties, shock and panic (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003).

Terrorists' attacks point to achieve effects on three sides. There is the direct infrastructure effect caused by cascading disruption or "*arrest of the functions of or key assets through direct attacks on a critical node, system, or function*" (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003); this kind of damage can be seen in the immediacy of 9/11 attack, that provoked instantaneous damage to facilities and services. The indirect effects show up when consequences arrive to government, society and economy through the reactions to suffered attack; an example could be the public disengagement coming after attack or massive disruptions. In order to counter-attack this kind of indirect effects it should be conducted an assessment of policy and regulatory responses, it should be understood the psychological response and an appropriate cost-benefit analysis of responsive actions. As another kind of attack there is the exploitation of infrastructure in order to strike or destroy another target, this is one of the most difficult attacks to prevent and also determine cascading and cross-sector consequences on the entire society.

As it is shown, modern society is highly dependent on critical infrastructures that provide goods and services. In times of divergence among states, these infrastructures are the first objective to be attacked and destroyed (Anderson, Fuloria, 2009) in order to spread panic and tactical disadvantage.

Therefore, protection and security is become a constant concern for governments. Moreover, an emerging consensus states that security and protection is a matter of business models and regulation, mirrored by the new branch of security economics, than of technological advancement. The next question to be answered is who is in charge of protecting these infrastructures

that are mostly privately owned but that have significant and persistent tactical value for governments?

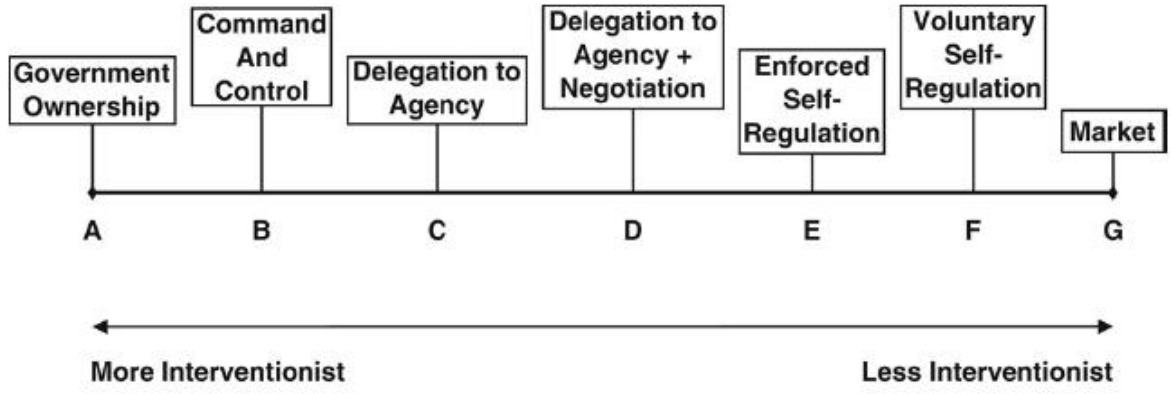
1.3.2 PROTECTING CRITICAL INFRASTRUCTURES

Critical infrastructures are so deeply bound to society and its functioning that any disruption or threat to their status could affect any activities and could also be a risk for human and environmental life.

The cases previously presented of large malfunctions of infrastructures and many others of vicious nature, which brings to mind 9/11 attack, bombings in Madrid in 2004 and in London in 2005, make clear the urgency of providing an effective and efficient protection to these systems, which are so fragile to numerous forces.

In order to properly assess vulnerability and risk, it is opportune to define what threat and risk is. According to American Petroleum Institute (American Petroleum Institute and the National Petrochemical & Refiners Association, 2003) a threat is" *any indication, circumstance or event with the potential to cause loss or damage to an asset*". A risk is defined as "*the intention and capability of an adversary to undertake actions that would be detrimental to U.S. interests*" (Roper, 1999). Starting from these definitions, it must be included other characteristics that distinguish threats, like the type, which could be insider, terrorist or environmental, the motivation and the triggers that might kick the start of the attack, the capability, methods and past trends of the attackers (Moteff, 2005).

Figure 1.4: Regulatory Continuum



Source: Assaf D., Models of critical information infrastructure protection, International Journal of Critical Infrastructure Protection, Volume 1, Pages 6–14, December 2008

Governmental intervention in Critical Infrastructure Protection can have many aspects and different approaches, often related to national interventionism approach. Therefore, as shown in Figure 1.4, intervention can range from total intervention to complete self regulation passing through some kind of partnerships (Assaf, 2003).

The most interventionist approach is represented by point A in the Figure 1.4, and it stands for in-house provision of CIP thanks to government ownership of infrastructures, this supposes taking full responsibility of protecting critical infrastructures that would lay completely on government. At point B of Figure 1.4, there is command and control regulation that assumes that government, through clear policies, gives cyber security standards and monitors and, if necessary, enforces these standards thanks to penalties. In this case, it is foreseen a slight relationship with private sector, even if its actions are limited by government legislation. Point C could be seen as a less strict control of government than command and control at point B, since legislation power is delegated to public agencies, which have discretionary powers in order to set fair standards because of their major expertise and their independency from political forces. The left side of the spectrum, containing points A, B and C, represents the highest degree of intervention by the state power over the markets, which comprehends rule-making powers, monitoring and enforcement of standards. This implies that responsibility for CIP is government's issue, while private actors have to accomplish to set rules.

Point D introduces negotiation among public agencies and single firms in order to achieve a compromise that makes possible and easier cooperate with government for common objectives. This approach can be well seen by markets, since it receive greater acceptance of cooperation from businesses, and it does not undermine the discretionary power government retains. In point E, the role of government changes and becomes more facilitative. In fact, rule-making power is given to private sector, and over this power it is up to government to oversee. Voluntary self-regulation, in point F, prescribes that standards are developed and enforced by private entities, with little government involvement. It works thanks to trade association that can require members to comply with standards (Aviram, Tor, 2004). The far right point G represents the market and the idea of self adjustments in order to reach optimal objectives. Therefore, the role of government is really limited in encouraging market solutions for CIP; it provides a stable and clear legal framework in which markets can act safely. Market will be driven by consumer's willingness to pay for reliable and resilient products and services, which would foster investments in protection and resilience fields, triggering competition among firms. As it has been shown, the right part of the spectrum requires a certain degree of trust on market power, and it needs a flexible cooperation among private and public actors.

Governments now have programs intended to protect critical infrastructures, but any of them have developed different approaches according to national interventionism philosophy (Anderson, Fuloria, 2009). In Europe national security represents a state responsibility, which is dealt with by government individually (Lewis *et al.*, 2013).For example, UK has brought regulation aimed to raise awareness toward protections and security topics. By becoming more discerning, security managers can put more and better-directed pressure (Anderson, Fuloria, 2009) on control systems.

However, it passed a European directive 2008/114 that tries to unify the assessment and protection of critical infrastructure. The aimed scope is restricted to energy and transportation, but it left the extension as the next step, starting from information and communication systems. This directive aims to

establish a secure network in order to facilitate member states to alert each other of threats to critical infrastructures.
The network, called European Reference Network for Critical Infrastructure Protection (ERNCIP), is founded on already-existing laboratories network, minded as a long-term and sustainable grouping (Lewis *et al.*, 2013). Its objective is to foster cooperation among different actors and numerous nations, in fact it supplies advanced technical capabilities, based on past experiences and capabilities of EU member states.
It works and it is successful thanks to the building of a reliable data set, which is easily used in making policy decisions. For this, confidentiality and trustiness are also addressed by ERNCIP as sensitive data collected in data sets would be needed to be exchanged and stored.

Until mid-2010, eighteen countries accepted the network view and adopted it, the list includes: Austria, Bulgaria, the Czech Republic, Denmark, Finland, France, Germany, Hungary, Italy, Lithuania, the Netherlands, Poland, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. In fact countries' representatives agreed that competences in order to effectively protect critical infrastructure are sufficient and robust, but these capabilities are difficult to be located and addressed. So the creation of data sets would make easier sharing information among states. Nevertheless, there are still small differences in assessing threats, even if all nations adopt an all-hazards approach, that means including all threats and risks irrespectively of their origins, in fact, some countries put more emphasis on natural hazards or terrorism pointing them as more important topics to be assessed.

A similar "libertarian" approach to European one is from OECD. Indeed, the organization tends to give key points and to be super-partes, it collects and produces documentation in order to give trigger to national debates about security and protection and it raises awareness of these problems within governments, business and private citizens (Brömmelhörster *et al.*, 2004).

In US Critical Information Infrastructure Protection (CIIP) has been aimed in order to promote partnership among government and infrastructure owners and

operators by increasing information sharing related to threats and vulnerabilities of critical systems (President' s Commission on Critical Infrastructure Protection, 1997). At the beginning of this process, government tried to promote voluntary self-regulation for sectors and to establish information sharing based on private-public partnerships (Dunn, Mauer, 2006), moreover it left to private sector the responsibility for developing CIIP standards, like access control, incident response and recovery plans.

Thanks to Clinton administration, the status of critical infrastructure protection was reviewed leading to the creation of President's Commission Critical Infrastructure Protection (PCCIP). Its objective is to reformulate the philosophy of protecting critical infrastructures through a national security lens and its way is to better understand the Information Age and the dependency on information and communications system. This commission widened the partnership among private and public entities, since representatives from AT&T, IBM, the Association of American Railroads and Pacific Gas and Electric Company sat on the commission alongside with government representatives (Givens, Bush, 2013).

Unfortunately, the commission work had resulted as inefficient face to a more challenging world, leaded by devastating terrorist attacks. Therefore, in 2002 the US government created the Office of Homeland Security (DHS) that is in charge to focus on resilience rather than mere protection. This change in objective, that is ensure that critical infrastructures are enough resilient, involves a stricter relationship among private and public actors, involving also general public in activities aimed to enhance resilience (Givens, Bush, 2013).

For instance, New York Metropolitan Transportation Authority launched in 2003 an awareness campaign, called "*If you see something, say something*", that encouraged people to report to authorities suspicious behaviours in order to support critical infrastructure resilience. Moreover, US government encourages citizens to be prepared for disasters, by preparing a family emergency plan. This preparedness could be easily translated into a macro societal awareness, which can help to improve emergency services and their response.

However, because of global financial crisis, businesses tend to diminish costs and therefore they cut security costs. Because of reduced budget, availability

and infrequent major disasters, a false sense of security emerges and leads to "*organizational apathy*" (Givens, Bush, 2013) in the medium-long run.

Protection issues are not just limited to engineering design systems, but embrace topic of legacy systems, the difficulty to understand strategic threats, the need for training and information sharing. In order to face properly critical infrastructure protection, it must be acknowledged numerous challenges that will improve security. First of all, it has been noticed a limited pool of resources available in order to address security problems, this can make worse the understanding and the acquired knowledge of control systems and that can increase risks and inhibit businesses. Then, the lack of sharing news about threats and incident among government and private actors can increase the risk of attacks because there is a sense of unpreparedness among actors. This is also the result of difficultness of establishing effective partnerships between government and businesses. Moreover, it results chaos and inefficiencies created by poor coordination among public agencies. Furthermore, the increasing sophistication of tools and methods used by hackers worsens the fastness of response and its efficacy.
These challenges should be resolved in order to make security valuable and efficient thanks to security economics rather than "*purely technical projects*" (Anderson, Fuloria, 2009). In fact, it must be found out how to implement sustainable and effective engineering solutions in different business environments, in order to become adaptive and preventive solutions.

Even if CIP would be better implemented with setting an effective partnership among private and public actors, there are also side effects that policymakers should take in consideration. In fact, there must be found a legal agreement that can benefit both parties. Contracts, for example, while useful, are essentially imperfect tools which establish a solid partnership on, since they cannot foresee unexpected issue and unpredictable but useful terms that may arise during the completion of duties required by the contract. This situation may present different solutions, ranging from accepting the new terms, negotiating the promise beyond new terms, or refusing the new issues. And, even if

contractors may be legally forced to carry on the contract, the situation that arises results in increasing expenses and lack of trust in the other actor.
Moreover, it is present a general and overcoming tendency to act out of pure self-interest without any regard for the partnership (Givens, Bush, 2013). The created tension between individual and collective objectives can affect the choices undertaken in critical infrastructure protection, bringing to the tragedy of commons (Hardin, 1968). A growing phenomenon is rising in partnership and it is free-riding (Kameda *et al.*, 2011). Therefore, actors tend to invest less in the partnership and doing this they maximize their gains and benefits. This influences choices to be done, since, in a partnership, an actor would be less incentivised to invest properly, he will invest the minimum amount required to sustain the partnership.
These behaviours diminish incentives to enhance coordination among private and public entities, as coordination seems to be effective and in place. But, this lack of incentive alignment induces stagnation in coordination of actions and, at the same time, lock in lower levels of security (Givens, Bush, 2013). These harm deeply CIP strategies, making partnership useless and inefficient.
Other challenges that CIP is facing is the ongoing underinvestment in protection measures because of financial crisis, this underinvestment highlights the need to prioritise certain sectors which are more vital or less resilient to hazards. Moreover, governments or private sectors do not understand or quantify the right amount of investments that critical infrastructure protection requires in order to be efficient. This misunderstanding is influenced by the lack of business cases, which can be analysed and can be the base for investment projections, and by the unknown long-term impact of CIP on society and economics (Hammerli, Renda, 2010).

Countries are known to follow three general trends about CIP that are analysed by Focal Report 1 Critical Infrastructure Protection (CSS, 2008). As it has been seen, there is a growing focus on resilience rather than mere protection and therefore an all-hazard approach, in order to protect properly the larger part of critical infrastructures. This first trend dictates the move toward a broad and comprehensive approach to protection, thus it needs to organize response plans to a wide spectrum of threat, either natural or human. This can ensure that

prioritized infrastructure are well protected thanks to resiliency and emergency plan and strategy, and at the same time, that other infrastructure are basically resilient to most of attacks or damages. Another trend is the increasing value and importance of cyber dimension of society, bringing alongside the awareness that information and telecommunications systems are particularly vulnerable and less robust to attacks. This cyber dimension issue has been always on the agenda of governments, since technologies and information are always more central in national strategy. Nowadays, governmental efforts are to protect information and telecommunication infrastructures by securing these networks against possible intrusion. NATO and Cooperative Cyber Defense Centre of Excellence, created in 2008 by the cooperation of Germany, Italy, Latvia, Lithuania, Slovakia, and Spain, is focusing on conflict-related aspects of critical infrastructure and ensuring better protection and resilience. In fact, numerous and harmful attacks to critical infrastructure have showed their vulnerability and their need of protection and investments in order to diminish the probability of disruptions and external unauthorized penetration to sensitive data and information.

The last trend represents the centralization of responsibility that is growingly a responsibility of governments. Society awareness about the importance of critical infrastructures and the holistic approach to identify threats and risks makes CIP so fundamental that public agencies can better assess infrastructure status and the required investment.

"*In order effectively to protect critical infrastructures ... countries must protect critical information infrastructures from damage and secure them against attack*" (G8 Justice & Interior Ministers, 2003). This means that CIP is a primary objective to be assessed by government, plus the cooperation with private actors who own 85% of critical infrastructures.

Therefore, it is essential to plan an accurate strategy in order to perform an immediate and effective response in case of disruption. This strategy is a mix of preventive actions (Hammerli, Renda, 2010) and remedy actions in order to balance the negative effects of a possible downturn. So, it must include prevention actions and early warning signals recognition patterns, it must be put in place an effective detection measures for threats and risks. Applying

these measures ensures a timely and precise reaction to any kind of failure that could occur.

Thanks to US experience, six phases have been recognized that are spread all over the event cycle. These phases help to better understand and prepare measures that prevent or contain failure effects.

In phase 1 there is analysis and assessment of assets and functions that are the basis of infrastructures, as well as vulnerabilities and interdependencies that can change the strategy approach. It is assessed, also, the possible loss or degradation of these infrastructures in order to analyze many scenarios that can actually happen. Therefore, thanks to these phases, it is possible to determine and value a proactive strategy, which can involve intercepting or disrupting attack or threats, either pre-emptively or in self-defense (Hammerli, Renda, 2010).

Then it comes to remediation phase that prescribes precautionary actions that must be taken before an event occurs. This leads to fixing known vulnerabilities that can be used by attackers or that can make the infrastructure less resilient.

Phase 3 is indications and warnings, which take place before or during the triggering event, in order to assess assurance capabilities of infrastructures and to determine if the event is to report. All these actions are in the sphere of preparatory measures, which are based on tactical and operational level information, which come from asset owners, critical infrastructure sectors, allied governments and intelligence.

In response to warnings and indications it starts mitigation phase, in which asset owners, intelligence and other operational and tactical level actors, take action in order to minimize the impact of failure or loss of infrastructures.

Phase 5 is incident response; it comprehends activities and strategies that are aimed at eliminating the source or the cause of the event, in order to lower probability of another attack or failure.

The last phase is reconstruction, which represents the last step of CIP life cycle. Its objective is to rebuild and reconstitute critical infrastructure capability and functions. This the most delicate phase, which need massive investments, and the most challenging.

However, this one-event life cycle is not representing all the difficulties and the reality since it often happens concatenated events which bring to crisis life cycle. This more holistic and realistic approach to events and accidents deals with actual consequences when they occur, by taking into account numerous events that happened or that are probable to take place, and it tries to focus only on relevant issues that can make arise problems from practical proceeding aspects (Hammerli, Renda, 2010).

Even if progresses have been made by governments and private actors, CIP is still a big question mark, that make wander if it has been reached an optimal solution to this problem. In fact, first of all there is an attribution problem, which means: who should invest in CIP?

Since, as it has been shown, many alternatives are possible, that range from government's duty to some sort of cooperation and partnership among government and private businesses. Then, the problem goes to how construct incentives in order to make critical infrastructure well functioning and resilient during all their lifetime. So free-riding and tragedy of commons problem must be properly addressed. The crisis life cycle shows that the lack of business cases, in which causes and response actions are analyzed, makes CIP a theoretical topic, with few correspondences to real situation.

All these problems must be addressed and resolved in order to properly protect critical infrastructures, which are so vital and fundamental to entire society and economics.

Chapter 2

CRITICAL INFORMATION INFRASTRUCTURES

Chapter two investigates in critical infrastructure particularities which are Critical Information Infrastructures. These are the base of many other critical sectors, linked with strong interdependencies and nebulous boundaries as Internet and telecommunications technologies (ICT) improve and enter daily life with numerous and different applications.

In **The governance of Internet in the Information Era**, it will be shown the various application of Internet and the growing importance of IT infrastructures and the focus on their resilience and security. In fact, well-functioning and secured Internet and ICT ensures the functioning of the overall economy and society, as they represent the platform for many other critical infrastructures.
Critical information infrastructures (CII) are more sensitive to external attacks and technological vulnerabilities, which can be easily exploited by malicious attackers. In fact, Internet is by design open and exposed to threat but at the same time leaves room to improvements and reducing vulnerable points of access, in order to improve and boost resilience and robustness of Internet and consequently of all other critical infrastructures which rely upon.

Risks for Developed Technologies shows the increased risks society and economy are exposed due to prominent use of Internet and ICT, such as physical vulnerabilities and risks of shutdown of critical operations and networks due to a too heavy traffic burden, then due to the increased interdependencies that connects numerous and different areas which increase the risks of spreading failures and damages. What puts more danger of failures on CII is the increased use and openness of Internet through Internet of Things, smart grids and industrial control systems, which increase vulnerable points and threats for the overall infrastructure of Internet.

In **Critical Information Infrastructure Protection**, the chapter ends coping with the solutions and recommendations in order to protect critical information

infrastructure which are by design and construction insecure and vulnerable, especially to attacks. Therefore, policy-making procedures should focus on preemptive actions and intelligent analysis in order to prevent and reduce always more damages and response time.

Chapter 2

CRITICAL INFORMATION INFRASTRUCTURES

2.1 THE GOVERNANCE OF INTERNET IN THE INFORMATION ERA

Internet and its application improves everyday life, thanks to its numerous usages and its wide network linking many others infrastructures and tools. The spread of massive and omnipresent Internet is clear when light is turned on, when smart phones can have access to numerous information, like traffic conditions, weather forecasting, when through tablets and smart phones it is possible to access data stored in office PC, when home equipment, like dishwashers, clocks and ovens, can help with time management and other advices thanks to Internet connection.

In fact, there are growing trends about technology and information that are revolutioning usual business routine thanks to cloud computing and M2M, *i.e.* machine to machine communication, that, alongside with more complex control systems like SCADA and other software, control electricity traffic and waste management.

Since IT systems, services and networks form a vital linkage among IT infrastructures, Europe focuses on its resilience and security, because economy and society welfare lay upon the well functioning and secured Internet and other IT infrastructures. Indeed, these infrastructures are aimed to provide and help supplying essential goods and they support as platform many other critical infrastructures (EU Commission, 2009).

Therefore, these facilities are managed as Critical Information Infrastructures (CII), since "*their disruption or destruction would have a serious impact on vital societal functions*" (EU Commission, 2009).

In US the Department of Homeland Security gives a round definition of critical information infrastructures, defining them as "*any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video*" (US Department of Homeland Security, 2012), that is essential and vital to the

functioning of other critical infrastructures and to the nation that, if it happened incapacity or damages of these infrastructures, there would be strong and unbearable impact on security, economy and public health and safety. It includes any infrastructures that correspond to this description may it be owned by or on behalf of government and local institutions. This American definition pictures a wider status of CIIs than European's, since it highlights the cooperation, voluntary or not, between private sectors and public institutions.

Adding to these definitions, NATO defining CII as a narrow concept (Lord Jopling, 2007) which identifies data flows and the networks through which information are sent. This splitting notion is essential to understand the protection strategies, which will be exposed later on this chapter, as they focus on both protecting data and protecting the physical infrastructures.

Also OECD understands the criticality of these CIIs as they can" *boost economic performance and social well-being and strengthen societies*" (OECD, 2008). CIIs are identified thanks to three indicators that point their criticality to nation, which is if IT components support other critical infrastructures, or support vital components of governmental concerns or it is basic and essential to national economy (OECD recommendation of the council on the protection of critical information infrastructures, 2008).

In fact, OECD recognizes the revolution of Internet by transforming economy and society routines and practices; undeniably Internet represents an open and decentralised platform that can ensure cheap communication, higher collaboration, and improvements in innovation and productivity that boost economic growth (Màtl, 2010). It has been proved that Information and communication technologies (ICT) form innovation driver and they are responsible for growth in productivity; private users depend on ICT for many reasons, for work, for social relations, and need security and protection of their sensitive data; moreover governments rely more on eGovernment services, which help public administration to get closer to citizens, this therefore makes public sectors too heavily dependent on these new forms of technologies (EU Commission, 2009). As OECD expresses (2008), becoming Internet more pervasive, ubiquitous and therefore essential, it promotes new interactions among global economy, which is transformed in Internet Economy, which brings also some other side effects.

Despite Internet proved to be sufficiently resilient and robust to accidents and attacks (Trimintzios *et al*., 2011), Europe recommends policies aimed at strengthen confidence in CII, by increasing security and resilience since this proposed strategy represents the first defence against any kind of attacks and accidents. EU Commission (2009) forecasts a medium probability of 10-20% of CII breakdown in next 10 years, and estimates 250 billion € of damages to global economy.
In general, CIIs are considered to be inherently insecure, since they are mostly developed by the private sector, whose first goal is not security but competitive design. Therefore, because of the lack of intrinsic security of components, CIIs are based on instabilities and many critical points so failures in information infrastructures are expected (Dunn Cavelty, 2007).

These new technologies, however, create not few problems to Internet and other critical infrastructures. They highlight physical and protocol vulnerabilities and limitations, as well as vulnerabilities to attacks and security problems. Moreover, these new technologies supply and operate thanks to public-private partnerships (OECD Ministerial background report, 2008) and need to cross national borders, since IT marketplace is always more global and interconnected. Therefore, any negative accident can and does influence numerous other IT users, affecting both private and governmental usage of Internet and its applications. Unauthorised disclosure of confidential data and information, as well as corruption and theft of documents, and also disruptions and difficulties to retrieve IT resources are all potential negative accidents that can have a strong repercussion on global society (OECD Ministerial background report, 2008).

The interconnected ecosystem of Internet includes the networks and their small parts that form the Internet. This comprehends numerous interdependent layers and connection points and delineates the open and decentralised architecture that characterised Internet (Trimintzios *et al*., 2011). This structure highlights and does not prevent some risks that instead must be faced in order to reach a better protection of CII and higher resiliency to attacks. First of all, there are technical vulnerabilities, when systems and services are disrupted in many

places at the same time and by the failures of other facilities; moreover, because of openness, ICT are easily targeted by intentional attacks. Then, there are economic concerns about ongoing business models, as fixed costs and competition drive prices downwards, and despite service providers have tools to make Internet resilient and better functioning, there is the potentiality of tragedy of commons. In fact, because of self interest behaviours, providers reduce their expenditures on these issues in order to limit the beneficial that other competitors may have from their investments. Same point for security strategies and investments that are stuck since it has not been found an incentive model to foster investments in this direction. Moreover, strategies of security and resilience are harmed by the poor quantity and quality of information about CIIs and their operations; therefore, there is a low assessment of resilience and of the status of CIIs and few projections of the impact of strategies or hypothetical accidents.

As far as now, many errors, mistakes and sins have been discovered thanks to rapid growth of Internet capacity and massive use. The strong interconnection and interdependencies of ICT upon other critical infrastructures and vice versa lead to bigger failure and congestions of large area, as from a single failure or a coordinated attack it is possible to originate regional failures or cascading technical failures, which spread malfunctions to a wider pool of users.

The Internet Interconnection Ecosystem is based on numerous connections that link different networks, through direct or indirect connections. These two kinds differentiate themselves thanks to different arrangements that rule the connection. It is direct when there is a bilateral and private arrangement (Trimintzios *et al.*, 2011), and it takes place usually under the control of both the involved networks. Otherwise, it is indirect when the connection happens thanks to incentives and bilateral agreements, either formal or informal. This kind of connection takes place more often since traffic flows through numerous networks covering the distance to the destination.

The Internet operability is ensured by a layered structure (Trimintzios *et al.*, 2011) which defines the grade of resilience of the overall structure. In fact, the resilience of each layer delineates and constructs the resilience and robustness of the architecture. Since the ARPANET (Hamill *et al.*, 2005) is the parent of

modern Internet, which evolves the definition of openness and flexibility, Internet relies upon routers and links and it is organised as Autonomous Systems which operates in order to address blocks of information to other machines and autonomous systems and to ensure the correct delivery of data. These connections form the physical layer on which communications take place.

Another basic layer is the network which has two main tasks, routing and traffic flowing. They are complementary. Since traffic flow is addressed to routes chosen by routing processes, by being careful of the effectiveness and the reach-ability of recipient machine.

Above these, there is the operational layer which groups people, processes and equipment aimed at monitoring the functions and operability of other layers. This duty is accomplished by autonomous system administrator (Trimintzios *et al.*, 2011) who is in charge of building and maintenance of network, of dealing with physical and equipment failures, of managing and adjusting network needs and capacity, in order to respond to demanded needs. A major problem at this stage is congestion, which can be located within the network, and therefore the administrator has tools to solve it, or outside the network, which is the more challenging to solve, as congestion negatively affects inward and outward traffic from the network, which creates buzz and discomfort.

The last three layers is commercial layer, which expresses business models and which measures traffic worth and price, then the economic layer, with incentives and drivers for players, and at the top regulatory layer, containing any rules that governs the overall system.

As Internet grows and becomes more challenging, the interconnected ecosystem can be stressed for changes in order to respond to a changing world and characteristics. Dynamics can be different between ICT and other critical infrastructures, like energy supply and crisis management and telecommunications, as it has been showed in chapter 1.1.2. Because of this highly changeability of Internet ecosystem, made through adding or removing connections, hubs or last-mile wire, there is little knowledge of the extension of ICT covered by incomplete and not accurate data (Trimintzios *et al.*, 2011). Moreover, it is not mapped physical linkages and their capabilities and

characteristics; there are few data about traffic volume and quality, and no clue about the routes that link autonomous systems, these absences give to Internet an aura of mystery.

Consequently, policy makers and engineers have to stimulate and support preparedness, security and resilience of CIIs, through national and European strategies in order to reach economies of scale and scope; otherwise the lack of cooperation among member states may preclude the success of any action plans (EU Commission, 2009). Moreover, it must be ensured the participation of private and public institutions and focus on their commitment and participation to the plan including all other stakeholders. Understanding the importance of ICT and in particular CIIs increases involvement sense and trust and security among institutions and citizens. Because of the growing number and sophistication of threats, due to technological advancements and because of increasing geo-political tensions (EU Commission, 2011), not forgetting climate changes, security and protection of these infrastructure is critical also at military level. Despite the malicious use of technologies, the omnipresence of Internet and other forms of telecommunications have improved the efficiency and effectiveness of coordination and cooperation (EU Commission, 2011) which ranges among multiple levels of stakeholders which makes living and pulsing the Internet ecosystem.

However, because of the increased use of technological achievements and due to global interconnectedness, attacks and failures tend to happen more frequently and provoke more damages than in the past, therefore there is urgent need of protecting these critical information infrastructures with a major focus on fixed and mobile communication and particularly on the Internet (EU Commission, 2011).

2.2 RISKS FOR DEVELOPED TECHNOLOGIES

Today it is always more prominent the predominance of Internet and society dependency on its use and applications. Thanks to powerful PCs and smart devices, users are increasingly connected through Internet.

This increased interconnection poses the problem of security and resilience of these new demanding networks, both physically and logically. The risks of man-made attacks and failures conjuncts with the high degree of interdependency of ICT and other critical infrastructures and with cross-borders interconnections (EU Commission, 2009). In fact, there is scarcity of knowledge about risks and threats that CIIs face, which, consequently, decreases the effectiveness of security plans. As it will be shown later in this dissertation, cyber-attacks and cyber warfare are real issues and, moreover, reach an unpredicted level of sophistication of attacks, hid behind profit or political causes.

Other vulnerability is the interdependencies (OECD, 2002) which critical infrastructures rely on, major examples of interconnection among ICT and critical infrastructures are energy supply, transportation and banking and finance, but nowadays, ICTs are essential and vital also in government services, SMEs and individual users. This importance is due to the increased capability of delivering information and instructions to and from all the critical infrastructures, which makes critical to society the presence of efficient ICTs (Clemente, 2013).

Therefore, because of this exponential growth of Internet and daily usages, information systems and networks are exposed to a wider range of threats and risks, which require and need security actions.

Physical vulnerability is due to the increased and selvage use of ICTs and because of increasing functional and quality requests. Therefore, physical infrastructures, who are not used to excessive demand, "*begin to blend into one another*" (Dunn Cavelty, 2007) and to spread cascading failures also to cross-border ICTs and critical infrastructures. This layer is influenced by the interaction between private and public sectors, as private organizations owns the 80% of critical infrastructures and operates the most. Different incentives

and payoffs stress actors to act not efficiently and drag them to behavior not-optimally for security and resilience of infrastructures (Clemente, 2013).

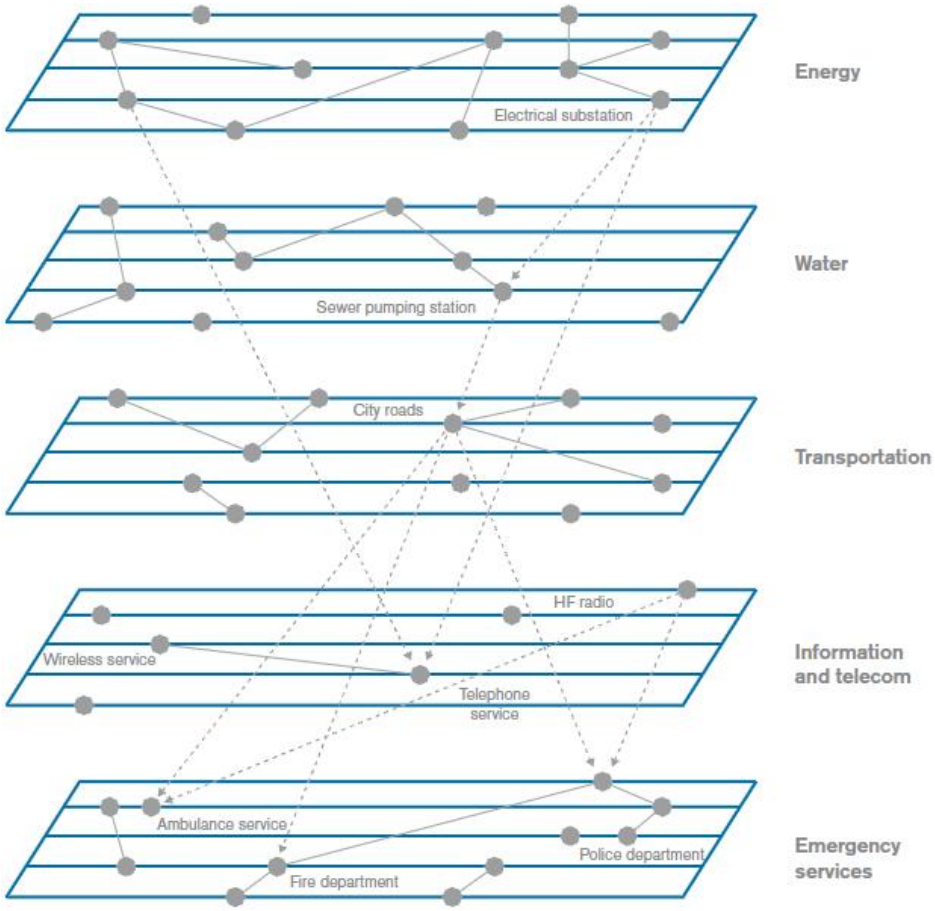
Since most of critical infrastructure is controlled and to a certain point managed by technological systems, the cyberspace becomes a focal point for the well functioning of critical infrastructures. In fact, cyberspace represents the evolution of social interactions, therefore it is a tool that augments communication channels and evolves the characteristics of social relationships and influences (Morningstar, Farmer, 2003). Because of this characteristic, cyberspace is considered to be the nervous system (Clemente, 2013) of critical infrastructures, since it connects them in order to communicate and give feedbacks. Despite the technological advancement, resilience is still a concern as critical infrastructures depend heavily on IT systems, which are usually outsourced by other nations. Consequently, resilience gains the spotlight as international links increase and critical infrastructures are always more dependent on IT networks.

Countless links between critical infrastructures and cyberspace exacerbates the challenge behind critical infrastructure protection, including and focusing especially on critical information infrastructure protection.

According to Dunn Cavelty (2011), because of the geographical expansion and the extension of provided services, the complexity of integrated network increases and does further due to the introduction of new devices and software with "*richer functionality using diverse technologies*" (Clemente, 2013).

Due to the increased economic pressures and a global supply chain, the knowledge and understanding of the dynamics implied in the interdependencies between critical infrastructures and IT. As said, the cross-borders location and ownership of critical infrastructures is an actual concern for European Council, that promotes coordination strategies at European level in order to limit "*transnational risks of interference"* (European Commission, 2011b) that originates disruption in more than one nation.

Figure 2.1: Infrastructures interdependencies



Source: Pederson P., Dudenhoeffer D., Hartley S., Permann M., Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Idaho National Laboratory, August 2006, [accessed 29th March, 2014] http://www.inl.gov/technicalpublications/Documents/3489532.pdf

In Figure 2.1, it is possible see the various and intrinsic interdependencies that bind all critical infrastructures and in particular shows the importance of ICT networks with respect to the functioning of other infrastructures.

According to Clemente (2013), there are five classes of international interdependencies, which have to be monitored and properly managed. The first is physical interdependency, which is explained by mechanical and engineering dependence on shared components; then informational interdependency expresses an informational requirement needed by other parts of the network; instead, the geospatial interdependency exists exclusively because of physical proximity of components; policy or procedural interdependency is due to the reaction in one nation's critical infrastructure to a change in policy or procedure that affects directly the original nation

infrastructure or component; the last is societal interdependency which describes the effect of event occurred to an infrastructure on societal factors, like public confidence and opinion and cultural issues. These represent the complexity that society and economy is facing right now, and that need to be behaviorally understand in order to model an efficient strategy (Pederson *et al*., 2006) to cover CII and critical infrastructure from risks.

These complexities derived by physical underinvestment and strong international interdependencies with critical infrastructure give reason to man-made attacks, since IT can be easily an entry point due to its vulnerabilities (Dunn Cavelty, 2007). What is challenging by facing this kind of threats is the unknown that covers the attacks and the attackers, since it is difficult to discover the provenience of the attacks and the reason behind it. The attackers range from inexperienced teenagers to expert hackers, going through terrorists and nations. Because of this heterogeneity, they are grouped in two categories based on the organizational complexity, on motivation and on resources (Dunn Cavelty, 2007), therefore, the unstructured group is a relatively limited threat, since it has counted resources and short-term goals, limited to the emotional sphere or aimed at profits, often lacking of persisting motivation. Instead, the structured group presents a methodical approach, backed with reasonable funds and professional support. Moreover, it is pulled by long term goals with specific strategies and strategic plans in order to achieve the maximum result from the attack.

The growing technological trends are driving more individuals to be connected to Internet in many new ways. It is estimated that in less than ten years it will be reached 50 billion of connected tools (Hesseldahl, 2011). This is a credible projection as new uses of Internet is progressing right now, as Internet of things is taking off and also cloud computing is always more intrinsic in business practices.

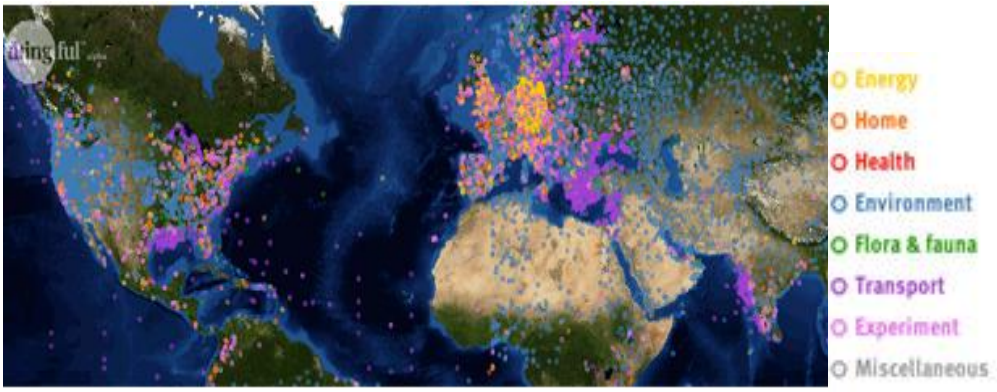
The potentiality of these technological advancements is enormous as it is mixed with human creativity, but at the same time they represent the largest threat to security of critical infrastructures. Therefore, there is urgent need to shape an efficient strategy that can appoint responsibility and accountability for

investment and decision making processes over these sensitive infrastructures (Clemente, 2013).

Industrial control systems are to command and control networks and systems with primary aim at supporting industrial processes, such as gas and electricity supply distribution, oil refining and distribution and railway and motorway transportation (ENISA, 2011 b). The most utilized industrial control system is SCADA system. Because of the wide expansion of adoption of these systems, SCADA is facing many incidents and cyber attacks showing the sensitivity of these systems. These systemic vulnerabilities are due to lack of authentication protocols and encryption systems, exposing SCADA communication to attacks, like Stuxnet and Night Dragon showed, hijacking and other cyber threats (ENISA, 2011 b). Nowadays, however, thanks to designing of IP-based industrial control systems, interconnectivity and efficiency is improved, benefiting the overall society and other critical infrastructures.

New devices called Internet of things are the last frontier of technology embedded with sociability, as they are programmed to exchange, aggregate and extract information from network. They can be any tool, from smart phones and PC to house equipment, like washing machines and ovens, to energy monitors, weather stations and pollution sensors. All these are constantly in communication with the Internet through autonomous connections (Clemente, 2013), thanks to M2M technology, *i.e.* machine to machine communication, that allows constant process of capturing, processing and sending data via network.

Figure 2.2: Map of the Internet of things



Source: Thingful, http://thingful.net/ [accessed 30th March, 2014]

Essentially, the intelligent objects can feel and react autonomously to surrounding environment thanks to radio-frequency communication.
A comprehensive definition of Internet of things is expressed by Murer (2010), who defines it as "*an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment*". In this broad categorization, it is possible to delineate the characteristics of future objects, like "*blogjects*" coined by Near Future Laboratory founder Bleecker, and smart objects called "*spimes*" by Sterling, addressing object "*of unique identification, aware of its location, its environment, that initializes and auto-documents itself and launches data about itself and its environment in large quantities*" (Murer, 2010).

They are expected to simplify everyday life to citizen and businesses, but, despite the practical simplification, they exacerbate the criticality of cyberspace. For this, cyberspace is divided into three layers which aim to make functional the overall system by cooperating. The lower is the physical layer, which includes hardware and routers and other physical component, then there is the logical layer which is composed by software that runs the physical layer, and last the social layer, which represents the numerous and different interactions between users' avatars representing real people or machine, as in the case of Internet of things (Clemente, 2013).

It is assisted an evolution of Internet of things aims and definition, since previously it was considered as the new communication protocol of radio-frequency identification and barcodes, then it went through a connective goal, that is connecting any sensor, device or applications to the Internet, it is going to prepare a third wave of Internet of things characterized by cognitive approach which forecasts data reuse, hyper-connectivity leverage and interoperability solutions, making this new model more intelligent and malleable (Digital Agenda for Europe) .
The benefit of this new technology will be mirrored also in economy field, as it is predicted to generate billions of Euros, which can foster economic growth and lower levels of unemployment. Moreover, citizens will be enriched with augmented and richer interfaces that will simplify life.

Risks come from the misuse of these new technologies rather than from technology per se (Daskala, 2010). Consequently, it is essential to assess the protection of Internet of things network in order to be ensured of its resilience, fast and efficient response plan to events, better awareness of strengths and weakness as well as opportunities of development and threats, large quantity and better quality of available information for supporting decisions and reactions and an overall efficient and cost-effective network (Gorniak *et al*., 2010). Otherwise, if a complete assessment had not been executed, the risk would exceed the benefits coming from this technology. In fact, there would be established a dependency on an inappropriate network, this would open doors to different attacks, like intrusion and denial of service, and it would mean that communication protocols could be inadequate reducing interoperability of devices and therefore limiting the connectivity and usefulness of devices. Then, a poor assessment of conditions would cause a reduced security that would perpetrate a loss of privacy and confidentiality of information and data collected by devices (Gorniak *et al*., 2010).

The applications of smart objects range in many sectors, who are usually critical infrastructure sectors and that therefore arise more risks about security and resilience.

Despite finance and banking sector is not directly touched by this revolution, there are some indirect effects due to massive and growing e-commerce. In fact, thanks to always connected devices, e-commerce is on the move and constantly reachable. However, it requires a strong integration with financial systems for transactional issues, arising at the same time privacy and data protection concerns (Gorniak *et al*., 2010). This wider use of e-commerce and the respective sharing of financial information arises the possibility and likely of cyber attacks aimed at retrieving sensitive information stored in financial systems.

The transportation infrastructure, instead, is directly interested by Internet of things and sensors network, as it is spreading the use of traffic monitoring, signaling, communication with and between vehicles and other means of transport (Gorniak *et al*., 2010).

Also energy supply sector is revolutionized by Internet of things, as smart grids, balloons and other sensors demonstrate. These applications highlight problems in design, which means to solve interoperability issues due to use of many different kinds of devices, and to improve communication network (Gorniak *et al*., 2010).

Smart devices will be useful also in health assistance and caring, thanks to e-health and other smart application that will ensure the ubiquity of health treatments. However, this application presents large problems configured as data diversity and database failures (Gorniak *et al*., 2010), alongside with security of sensitive data that this service requires and needs. Interoperability among numerous and diverse devices needs to be addressed in order to ensure an efficient service. Moreover, it could present difficulties in qualifying service specifications, ranging from consultancy to a more complex and personalized treatment, and in overcoming society doubts about technology.

Even if each service presents different problems and issues to be addressed and solved, there are still concerns about resilience of these devices. First concern is about the capability of integrating a growing and important numbers of sensors and smart devices. Another issue is the robustness to unusual traffic distribution, geographically and timely speaking, that could downgrade quality of services. As already said, interoperability is the focal issue as different

devices are connected by heterogeneous systems (Gorniak *et al*., 2010). Furthermore, these networks build on smart devices are object of malicious attacks and devices aiming at influencing the interpretation of actual data compromising the processing and reaction of devices (Gorniak *et al*., 2010). Most frequent attacks is sinkhole attack, which proceeds by attracting to an altered node surrounding sensors and altering data flows, or throwing them away or launching further attacks (Gorniak *et al*., 2010). Then there is the replay attack in which "*the attacker records routing traffic from genuine routing nodes and uses it to create a topology that may no longer exist"* (Gorniak *et al*., 2010). Sleep-deprivation attack, instead, generates fake activity and data flow in order to discharge neighboring nodes creating massive difficulties to other nodes to communicate with superior level stations (Gorniak *et al*., 2010).

There are two interesting applications of Internet of things, the former are smart grids, the latter is cloud computing, that will be discussed later in this chapter.

In order to reach European Union objectives of cutting pollution by 2020 and to use more renewable energy and to increase energy efficiency, it is up to smart grids that can properly help to integrate new forms of energy with the ordinary ones. Smart grids are defined as upgraded "*electricity networks that can efficiently integrate the behavior and actions of all users connected to it - generators, consumers and those that do both - in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply*" (EU Commission Task Force for Smart Grids, 2010). They are resulted as an essential actor in reaching 2020 targets of the EU (ENISA, 2012a), as they can effectively integrate different forms of energy and deliver them to users and consequently their approach is user-oriented, as smart grids collect data of users consumption and react in consequence of these. Thanks to Internet of things and smart devices, smart grids will have access to better and more information, being able to put in communication energy suppliers and consumers and to improve the control of energy consumption (ENISA, 2012a).

Therefore, IT network is essential platform for smart grids communications, which demonstrates again the importance and the interdependencies that bind critical infrastructures and CIIs. This strict connection with ICT makes vulnerable also the smart grid system to malicious attacks (ENISA, 2012d). Consequently, smart grids in order to be a successful project adopted vastly need to address problems that limit their proliferation. An economic concern is the cost of producing and installing smart grids, not forgetting the costs of upgrading electricity networks. Societal issue is the suspicions of consumers, therefore it should address increasing awareness and guaranteeing privacy and protection of sensitive data (ENISA, 2012a).
However, smart grids increase the likely of attacks, since there is an integration of end user property as home-based energy sources, which extend vulnerable points threatening further electricity system (ENISA, 2012a).

The conjunction of smart grids and Internet of things in general brings to the building of smart buildings, a new form of civil engineering integrating sensors and devices sensible to internal and external environments. Thanks to this sensibility, smart buildings can adjust temperature, illumination, rationalize water and electricity, in order to respect sustainable parameters of consumption and decreasing pollution (Murer, 2010). A perfect example of smart building and eco-sustainability is the One World Trade Center, which integrates sensors and recycle systems in order to have the lowest possible environmental impact.
The next step are smart cities which are "*made safe, secure, environmentally green, and efficient because all structures -whether for power, water, transportation, etc. are designed, constructed and maintained making use of advanced, integrated materials, sensors, electronics, and networks which are interfaced with computerized systems comprised of databases, tracking, and decision-making algorithms*" (Bowerman et al., 2000). In few words, smart cities represent a new approach to the relationships between information and communications technologies and critical infrastructures, making these more "*aware, interactive and efficient*" (Belissent, 2010). Smart cities make conscious choices and effort in order to proactively reduce actual problems cities are facing, like traffic congestion, safety and energy waste. Therefore,

thanks to an innovative employ of ICT, it is possible to support "*a more inclusive, diverse and sustainable urban environment*" (Màtl, 2010).
Perfect example of smart city is Amsterdam and the project of reducing pollution by 40% and reducing energy by 20% in order to met the EU 2020 standards. It has been possible reach a great result thanks to strict collaboration and cooperation among citizens, businesses and government. Thanks to smart grids and other advanced technologies, Amsterdam adopted new approach to living, working, mobility and public space, each focused on economic and environmental sustainability (Brinkman, 2011). Acting like this, Amsterdam hopes to increase the attractiveness of the city by becoming more eco-friendly. However, smart cities encounter problems, ranging from the difficulty of political alignment and evolution, the important investment to undertake in order to make happen the progress, the time-consuming process of cooperation and to manage an efficient stakeholder involvement which made successful the Amsterdam case (Brinkman, 2011). Despite these problems can hamper the adoption of this approach to city governance, smart cities and smart grids are the answers to actual problems of daily life.

Cloud computing has been through life cycle of technologies with a starting booming expansion, then a disillusion phase that is finishing in these recent years, as it shows its value and importance in IT infrastructure. Cloud computing is a growing trend, as testifies the rapid adoption across society and the expected projected trend of 30% growth a year (Dekker *et al*., 2013). As adoption increases, cloud computing becomes more and more critical to many users and infrastructures that rely on it. In fact, cloud computing services are adopted by critical sectors, like finance and banking, energy supply infrastructure transport and government through governmental clouds (Cateddu, 2011). The growth and the sparse subscription of cloud computing services make cloud computing critical and essential to businesses and single users. However, this saturation of IT resources can result as a double edged sword, as an higher adoption of these services reduces costs and ensures a better security and business continuity, it can also result in a massive failure due to an outage or security breach unleashing a domino effect cascade of damages (Cateddu, 2011).

Cloud computing, despite the common thought, is not a new technology but it is a new approach to delivering IT resources and services, like data storage, software processing and email handling, that are instantly and on-demand available and reachable. Cloud computing offers three services and multiple settings to meet consumers' require. It can offer a SaaS, *i.e.* Software as a Service, which makes available third-party software on demand via Internet. It can be PaaS, *i.e.* Platform as a Service, which allows customers to develop new software and application using a remote connection, and it offers development tools and configuration management. Otherwise, cloud computing can be under the form of IaaS, *i.e.* Infrastructure as a Service, which provides complete packet of IT resources as virtual machines and other hardware and operating systems to run them.

Moreover, cloud computing can be configured as public, so it is openly available with no restrictions, private, which makes the cloud accessible only to private network users, or partner, which is hybrid configuration as it is accessible to limited and well-defined and recognizable users or organizations (ENISA, 2009b).

Thanks to the architecture, cloud computing offers numerous advantages and benefits also thanks to its large scale, which ensures appropriate investment in security and protection of infrastructure. As cloud computing providers start conquering more consumers, they benefit of impressive economies of scale regarding security actions, as defensive measures, acting on filtering, hardware and software redundancy, stronger authentication, which also improve the overall architecture by ensuring a higher protection and security to many users and critical infrastructures (ENISA, 2009b). Other benefits coming from economies of scale applied in cloud computing providing is the ubiquity of infrastructure, which creates the necessary and robust redundancy useful against failure and for an efficient level of recovery (ENISA, 2013a) (ENISA, 2009b); consequently to geographic spread, service reliability and therefore quality of service are improved and decrease the chances of major failure side effects, thanks to redundancy (ENISA, 2009b); it is possible to put in action a threat management by hiring specialists, benefiting all the users that cannot

afford such service, and this decreases response timeliness thanks to early and effective detection of failures or attacks (ENISA, 2009b).
Cloud computing architecture shows different advantages that benefit the entire society, in fact it reaches instant scalability and offers enormous flexibility to users, and it provides an on-demand service adopting a "pay as you go" pricing model (ENISA, 2009b).

However, cloud computing face many and a lot of risks and threats that take advantage of vulnerabilities. A loss of governance is required to client as he cedes part of control which is settled in cloud provider's hands, this may lower security level as it is controlled centrally by cloud provider (ENISA, 2009b). Because of lack of interoperability among procedures and tools provided by cloud providers and application and data, it is possible to notice a lock-in effect showed in the difficulty for clients to migrate to another provider or to in-house solutions, creating dependency over cloud provider, especially if data exportability is disabled (ENISA, 2009b). The likely of attacks of separation mechanism between storage, memory and routing processes highlights the isolation failure risk, which is, however, less probable and more difficult to attackers with respect to traditional attacks (ENISA, 2009b). Moreover, risks come also from customer management interfaces as they tend to increase risks due to remote access and browser vulnerabilities that can propagate to the cloud (ENISA, 2009b). The recurrent risks of CII are data protection and malicious attacks and access which are followed especially for cloud computing by insecure or incomplete data deletion. Clients must have trust of cloud provider and its processes of data handling that have to be legal and protected. In order to encompass this risk and loose customers trust and reputation, cloud providers should give information about their processes of data handling practices (ENISA, 2009b). A strong impact is due to legal dispute or investigations involving the provider or one of its customer over data of customers and the reputation of provider (ENISA, 2013a). Similar problem when a request of deleting or shouting down clouds is made and data are impossible to cancel or accessed, because they are not available or stored with other clients' data. This risk is predominant for those clients that rely on reused hardware resources or in case of multiple tenancies of hardware (ENISA,

2009b). Cyber attacks exploit cloud vulnerabilities for data breaches that affect simultaneously millions of users, as the impact of attacks is multiplied by the concentration of shared resources (ENISA, 2013a) which is the base of cloud computing philosophy and architecture. Fortunately, thanks to architecture and design of cloud computing, it is endowed of elasticity which is useful when coping with overloads and cyber-attacks (ENISA, 2013a).

The increasing recourse to Internet and its application shows beneficial aspects on society which benefits of improved quality of services and consequently of life, as well as a sustainable approach to buildings and constructions, and the ubiquity and always accessible data and information which helps especially businesses and governments.

However, this massive approach to ICTs makes critical all the infrastructures involved and which have strong interdependencies with. The recurring risks are data protection, infrastructure and architecture security, protection from cyber attacks and resilience and robustness against natural disasters. All these require investment on security and protection, making resilient to any sort of failures all CIIs, that are no more just PCs and fixed telephony but it includes smart phones, smart objects, cloud computing, sensors, emergency services, finance and banking system and energy supply. Therefore, the next step to be undertaken is to assess the security level of actual CII and to project an efficient security strategy in order to properly protect sensitive data and vulnerable architectures.

2.3 CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

As critical infrastructures need to be protected and secured by attacks or failures, more so need critical information infrastructures because of their enormous importance due to " *dense interconnections between sectors*" (Clemente, 2013). Due to this difficulty in identifying and distinguishing the boundaries of critical infrastructures, critical infrastructures go across every aspects of modern society and improve it.

Therefore, critical information infrastructures have to guarantee availability, reliability and resilience (Cukier, 2005) for the well functioning of any other critical infrastructure, this strong dependency over CII increases significantly importance of the protection of these information infrastructures. Even if CIIs support critical infrastructures' actions and work, it seems that CII have received less attention about protection with respect with other critical, and maybe more tangible infrastructures, most of the time protection is limited to terroristic threat, despite most of disruptions and failures occurred because of natural disasters, human error or inadequate public policy and investment (Cukier, 2005).

CIIs show to be inherently insecure due to their private belonging and designing (Näf, 2001), consequently informatics vulnerabilities are expected and foreseen, information networks' instabilities need to be addressed not only by design improvements, but especially by public policies.

Europe has addressed many communications over this subject of CII and its protection in order to ensure a pan-European approach and to balance efforts and investments (ENISA, 2011b). Communication 786/2006 titled "*a European Programme for Critical Infrastructure Protection*" gave a first approach to an European programme for critical infrastructures protection (EPCIP) and gave momentum to manage an European framework for protecting critical infrastructures. Moreover, it prioritized protection from terrorism threat, even if alongside with an all-hazards approach, due to massive cyber attacks of malicious nature that stroke Europe and other nations.

This is developed in the communication 149/2009 which treated specifically critical information infrastructure protection recognizing the important and

essential role of IT platform for other critical infrastructures and it defined a strategy in order to strengthen security and resilience of CII (ENISA, 2011b) . This strategy provides a five-pillar model based on preparedness and prevention, detection, response, mitigation and recovery (ENISA, 2011b), and integrating international cooperation and mutual aid.

The acute vulnerabilities of CII make them insecure and exposed to many threats and risks, among which terrorism is neither the most probable or the most dangerous attack that ICT face (Dunn Cavelty, 2007). Of same or worse impact on CII there are natural disasters, physical failures and misleading actions of authorized and unauthorized users (Dunn Cavelty, 2007). The overall infrastructure can be affected severely even if outage are temporally or geographically limited (Cukier, 2005). Despite causes can be of various nature, either intentional, accidental, because of poor quality decisions of designing, management or regulation, the majority of incidents and failures are due to natural disasters, human error and bad design (Cukier, 2005).

There are two main classes of threats to CII, internal or external, which causes immanent damages both economical and physical. The internal threat is defined as "*one or more individuals with the access and/or inside knowledge of a company ... that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm"* (Indian National Critical Information Infrastructure Protection Centre, 2013); this kind of breach provokes losses and damages because of IT sabotage, fraud and theft of confidential data and information, causing economical and reputational damages for the business. Instead, external threats come from outside the firm and it is acted by hackers, competitors, terrorists, foreign governments in order to cripple CIIs, perpetrate espionage acts, provoke cyber warfare or threaten with cyber terrorism (Indian National Critical Information Infrastructure Protection Centre, 2013).

Even maintenance operations may cause disruptions and temporally malfunctions, this is because CIIs are so complex and sensitive to any change in traffic or volume data that may result in a shutdown of services or general disruptions of infrastructures (Dunn Cavelty, 2007).

Therefore, resilience has great importance in these infrastructures and at international level, because, as already seen, numerous digital and physical interconnections create efficiency but at the same time it creates strong interdependency and dependency (Clemente, 2013). As disruptions can happen at any time and affect consistently many critical infrastructures at once, resilience need to be assessed and properly addressed by policies in order to sustain this working equilibrium among CII and critical infrastructures.
Thus, it must be enforced an active cooperation between private sector, which owns most infrastructures, and public area, there is need to offer adequate incentives which can properly drive investment and attention toward these infrastructures.

Consequently, greater stress is put on protection of CII, and more on the amplitude and magnitude of the intervention on protection. In fact, it is impossible to plan a strategy of protecting CII from all threats and risks because of technicalities and practical reasons and mainly because of immanent costs (Dunn Cavelty, 2007). Therefore, protection plan needs to focus on the most critical infrastructures, in relation to the possibilities of threat or attack and to costs of protection.
For these reasons, it is not possible, and highly not advised, to adopt an one-fits-all solution, but it should be adopted a tailored solution to specific threats and specific infrastructures. It should be, then, adopted an all hazards approach which is designed for protecting nonetheless of threat nature, but mainly focus on creating responsiveness capability to a wide range of unexpected events and risks thanks to greater resilience.
Moreover, protection plans need to have an international concept and focus, as vital and strategic parts are always more frequently located in other nations and because of global intrinsic nature of cyber sphere. However, even if international cooperation and private-public integration are known to be essential for efficient and effective protection plans, divergences in national CII protection (CIIP) are the first obstacle to be overcome, by converging national expectations and targets. In fact, it is essential in the IT sector that national protection policies are complemented by cooperative multilateral agreements, because in ICT national boundaries have little meaning and

relevance due to increased interconnections of CII (Clemente, 2013). Therefore, governments are trying to sign international conventions in order to give protection to "*global information environment*" (van Eeten *et al*., 2006). Other obstacle is the lack of private and public cooperation in CII protection, in fact CIIs are for the majority privately owned and international, but protection incentives are insufficient for a proper implementation of effective protection policies, as costs rely on businesses , while government do not clearly regulate CIIP creating buzz and chaos in investments (Cukier, 2005).

What is clear is that some changes are required by businesses and society, as expressed during Conference on Information Law and Policy for the Information Economy (2005). Since CII is by design decentralized, interdependent and controlled by numerous stakeholders, CII shows vulnerabilities that require a high degree of protection. It would need incentives and governmental regulation, as market forces cannot provide the sufficient and effective protection. But, at the same time, governmental efforts should be go alongside with private sector, as regulation on its own may not produce optimal results, since it does not take into account technical changes, and it could be too much focused on legal and forced compliance rather than security and protection. Governmental authorities are required to support protection activities "*by serving as an observer, providing antitrust immunity, and encouraging limited disclosure of risks*" (Cukier, 2005). Moreover, protection of CII open the road to insurance and its benefits, as it can smooth the progress of building a database for information aggregation and risk assessment, improving, thus, both protection and insurance policies. Insurance market can act also as incentive for best practices and creating a market for security, in which premiums and eligibility for coverage play important role in incentivizing protection and attention to strategic risk management (Cukier, 2005).

In Chapter 1.3.2, it has been showed protection strategy and objectives and challenges in order to protect effectively critical information. Between critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP) boundaries are weakening as interdependencies grow between physical

critical infrastructures and intangible cyber space of critical information infrastructures. This lead to interchangeable use of terms, coining the new comprehensive acronym CI(I)P (Angelini *et al*., 2013), since these two protection approach have peculiar qualities and points and show the urgent and practical need of more protection for cyberspace and ICT. CIIP is aimed to protect IT connections and network that links other infrastructure sectors, whilst physical components are protected by other protection measures (Brömmelhörster *et al*., 2004).

CIIP is, on broader terms, a framework in order to provide to nations a structured view of strategic information management (Wilke, 2007); it may represent an effective information sharing tool that picks information up about risks, threats and vulnerabilities and undertaken protective actions.

CIIP's aim is to protect "*communications or information service[s] whose availability, reliability and resilience are essential to the functioning of a modern [national] economy, security, and other essential social values*" (Cukier, 2005). According to NATO (Clemente, 2013), from CII definition as data flow and channels that are used to deliver data flow, CIIP is perceived and structured, consequently, as protecting and securing both data and privacy and information infrastructure (Lord Jopling, 2007). All around the world, nations try to catch up with OECD recommendations for CIIP, in order to build efficient and functioning protection plan, since ICT are sensitive for health, safety and security of citizens (OECD, 2008). OECD requires that CIIP constitutes a national policy based on cooperation among private and public players, with other critical infrastructure owners, and by forming coordination and cooperation agreement at international level. OECD suggests to nations to divide authority and responsibility among definite agencies and organizations that are to implement policies addressed to CIIP; it advises to get private sector involved in order to enable an efficient information sharing to ensure a better and deeper protection of ICT; in order to protect and ensure CIIs risk assessment and strategic risk management must be assessed, and it needs to develop an efficient incident response capability with recovery actions aimed at protecting CII capability.

Generally speaking, government has the responsibility of creating a favourable environment in order to build and implement CIIP. First of all, it is required to assist private players, such as owners and operators of CII, and to share information in order to enable a better protection; this cooperation and information sharing would help in identifying and understanding vulnerabilities and interdependencies (Wilke, 2007). The national efforts should go in the same direction of international CIIP organizations and actions in order to not counterbalance individual efforts, but instead strengthen their results. At the end, OECD (2008) advises to run tests and measurements of CIIP results and achievements.

In Australia, CIIP is considered vital to maintenance of society and to business survival, CIIP needs to assure physical stability and safety of key critical assets alongside with IT systems and infrastructures (Wenger *et al.*, 2002). In the Netherlands, CIIP is seen protecting the country, society and allies against disruptions or disturbances, either voluntary or not, of ICT infrastructures (Wenger *et al.*, 2002). In US, the focus is on reducing the frequency of disruptions, the duration of failure and that can be manageable (Moteff, 2002). The common trait of nations is the path of CIIP, which is supported by clear legislative actions, by cooperation at national and international level and other initiatives to make stakeholders sensitive to this subject (Wenger *et al.*, 2002).

In order to put in action an efficient CIIP, it is important to structure a clear model that can help operators and owners to identify and cope with incidents and failures of these sensitive ICT. CIIP is meant to reduce dysfunctions due to vulnerabilities, making CIIs more robust and resilient to disruptions and that "*any impairment is short in duration and limited in scale, and services are readily restored when disruptions occur*" (Juster, Tritak, 2002). The antecedent of five-pillar model described in European Communication 149/2009 (ENISA, 2011b) is the four-pillar model (Suter, 2007), which organizes systematically the operations to address in case of malfunctions and disruptions.

A great importance is given to prevention and early warning, first step of four-pillar model, while in five-pillar model it is given focus to preparedness and prevention (EU Commission, 2011a) aspects. Prevention is functional to businesses as it increases the capabilities and kwon-how for coping with

disruptions and other malfunctions. Especially for ICT prevention it should be focused on three main vulnerable aspects of CIIS, implementing preemptive actions against IT malfunctions, preventing expansion of failures, and, thanks to analysis of causes, preventing recurrence of failures (OECD Ministerial background report, 2008). Prevention is the base for properly implementing and ensuring an effective CIIP, as some elements of prevention are present in all the steps of the model (Suter, 2007). Preparedness is implemented thanks to partnerships aimed at ensuring an improved level of resilience, such as the European private-public partnership for resilience (EP3P), which is an European-wide framework for improving resilience of ICT by fostering the cooperation between public and private sector (EU Commission, 2011a).

As second pillar, there is detection in both the model, aimed at promoting security and protection of CII, it is dependent on new technologies and their capability to detect new and more complex threat in short time. Despite each business should be able to independently detect threats to ICT, it is fundamental at this stage to build national and international networks, such as Computer Emergency and Response Teams (CERTs)(Suter, 2007) and ENISA project European Information Sharing and Alert System (EISAS) (EU Commission, 2011a), which can ensure collaboration with technical experts which can detect on a timely basis threats to CII.

The next step is reaction and response to attacks and threats by identifying and correcting the original causes of disruption or vulnerability. This stage is bind to law enforcement and policy making approach to CII attacks, and less focused on technicalities. In fact, prosecution of intentional attackers acts as reaction and preemptive actions against other attacks, law implementation, indeed, can increase risk of capture, can make more rigid prosecution and wider deterrent (Suter, 2007). In mitigation and recovery, it is fundamental to analyze incidents reports and to share information and data over networks and partnerships, this boosts improving crisis planning and management (Suter, 2007). The reports about incidents and all the actions undertaken as prevention and reaction are useful for creating shared basic mechanism and procedures for communication among different nations and different players (EU Commission, 2001a).

In five-pillar model, there is also international cooperation, which is essential to implement effectively a protection against failures and attacks that can affect many users and spread negative effects across borders. International cooperation should, consequently, promote shared framework of principles and guidelines for "*international collective engagement on the long-term resilience and stability of the Internet*" (EU Commission, 2011a).

However, despite technology improves day by day, it also means that new vulnerabilities emerge and new methods of attacks are possible. Therefore, protection will never reach perfect coverage, as security technology tries to catch up. Despite it is stated by technologists that security and protection tools that could protect CII from numerous potential failures (Cukier, 2005), these new and more powerful technologies are not deployed or implemented, the causes are to be pointed due to economic issues rather than engineering difficulties. Indeed, economic concerns are the reasons of the laxative protection that is undergoing now, as it is extremely costly to run a complete assessment of threats and vulnerabilities. However, protection is a top priority for 40% of IT businesses (Cukier, 2005), spending on average 5% of budget on security and protection actions, while at worldwide level, it is spent €100 billion annually, showing a growth of 5-10% per year.

Therefore, the economic burden make questioning who should pay for implementing the most efficient protection plan. This choice is solved in two scenarios, joint-care or alternative-care. In the latter scenario, the burden is on one's party shoulders and it benefits every player. However, cooperation is essential, as already said, so the alternative-care scenario is not optimal. On the other hand, joint-care is based on precaution and prevention actions of each player, costs are shared and therefore risks decrease. The benefits of joint-care approach are decreasing marginal returns to precaution, community's immunity to sanctions by adopting preemptive actions. However, it is challenging to implement a cooperative approach such as joint-care requires, because of human behaviors to maximize private interests and minimize efforts. Though, market forces cannot be a solution to decide who is entitled to pay for protection, as it cannot relieve free-riding issues and egoistic approach to this problem, but joint-care collaboration can at least diminish the negative

effects of behaviors through incentives of cooperation and collaboration (Cukier, 2005).

Chapter 3

STRATEGIES OF PROTECTING INFORMATION FLOWS

Chapter three deals with the importance and value of information and data, which constitute the essential raw material for any business. As WikiLeaks has proven, the security and protection of sensitive information and data become a priority for organizations, which try to construct valiant models that could help business to deal efficiently with everyday operations and processes. Therefore, models and management strategies would be useful and indispensable for business in order to handle carefully these key assets.

In **Assuring Information to Mitigate Risks**, it is explained the urgent need of implementing new strategies of protection and assurance of these key assets, since digital life and the corresponding Big Data create an indelible record. This data can be analyzed and processed in order to retrieve useful information about consumption patterns, buying attitude and preferences.
However, at the increase of this retrievable data, security breaches and integrity attacks increase in quantity and in wideness of chosen targets, from single user to large business and governmental database. Attacks, in fact, tend to exploit information value by maliciously acquiring them or corrupting them in order to gain informational power or to weaken competitors' advantage.
Therefore, information assurance (IA) may provide appropriate levels of confidence over system security and critical assets. Information assurance provides a holistic approach, which includes scientific, technical and managerial capabilities in order to efficiently protect and defend information systems and flows.

Applied Models of Information Assurance describes synthetically and analytically the most famous and utilized models of information assurance. These models improve the availability to decision-makers of information and data when they need it, moreover models assure that data are accurate and complete and ensure that control over these assets is ensured and maintained. Information assurance ensures the highest detection capabilities, if loss of

control over information process takes place, and it ensures recovering capacity and it helps restore IT system in order to keep data and information integer and secure. Proactive actions and strategies are suggested in order to set protection measures and put into action defence measures by integrating secure technologies and best practices.

In **Managing Risks and Information Strategically**, it is showed how increasing risks due to high reliance on IT resources are emerging and threatening organizations, which are translated as increasing of costs and weakening of robustness. Therefore, it should be applied a strategic risk management, an iterative process for identifying, assessing and managing all kinds of risks and uncertainties in order to protect activities and data. Putting in place programs aimed at managing and mitigating information assurance risks is a right move for organizations to be prepared for any circumstance. In this chapter, it is highlighted the need of strategically and structured managing information, thanks to information management, which is the collection and management of information flow. The symbiosis of information management practices and IA models would be able to ensure an efficient fruition of information and data, improving practically the quality and quantity of operational decisions.

Chapter 3

STRATEGIES OF PROTECTING INFORMATION FLOWS

3.1 ASSURING INFORMATION TO MITIGATE RISKS

Nowadays information is the base of power but, in the meanwhile, can be the greatest vulnerability of business and governments. In fact, data and information are the driving force in economics branches, like marketing and pricing, but also in politics, thanks to massive use of analysis, and defence issues, like WikiLeaks had shown.

The increasing appeal to digital world has created "the *first generation of humans to have an indelible record*" (Schmidt, Cohen, 2013). Digital life, indeed, leaves a digital signature ready to be analyzed and used for numerous different aims. Moreover, Big Data play a great role especially in US politics and social issues. From digital signatures, thanks to deeper analysis, greater amount of information coming from phone calls, e-mails and Internet searches, but also from social network relationships, is used to predict and prevent dangerous events, managing disasters, essentially to observe citizens and their habits (Zakaria, 2013).

Even if the objectives of data analysis are benign for society, the protection of this sensitive information should be essential and well implemented in order to keep safe all the power that derives.

Strong dependencies and interconnections created by Internet and telecommunications tools highlight vulnerabilities that are rapidly exploited by criminals or intruders. Thus, computer security breaches, alongside with confidentiality and integrity attacks, are increasing in number of attacks and in spread of targets, from businesses to governments (Colwill *et al*., 2001).

Therefore, companies and their networks are always more exposed to threats and risks for their retained information.

In this vulnerable setting, information assurance is fundamental in order to provide appropriate levels of confidence over system security and critical

assets. Attacks would exploit information, by acquiring or corrupting them, in order to gain informational power or to weaken competitors.

Protecting systems have been through technological evolution started in the fifties, and it mirrored technological advancements made in the latest years (Antinori, 2011). One of the first technologies implemented was Communication Security (COMSEC), it was essentially based on cryptography and its benefits, and it is used for classified and unclassified military documents. Instead, Computer Security (COMPUSEC) is structured over the protection of interchanged information processes, which characterize Internet networks. The next evolution is INFOSEC, *i.e.* Information System Security, which is born because of defects of the previous technology. In fact, COMPUSEC had difficulties over management and storage of information which indicates a new approach to protection of informatics employed at a higher level.

From this last INFOSEC, it gets to information assurance which is aware of the complexities of IT processes and the growing need for a systematic and contextual protection through the entire phases information pass through, which are transmission, elaboration and storage of information and data.

According to IAAC, information assurance Advisory Council, which is to ensure a robust, resilient and secure foundation for information assurance in UK, definition of information assurance represents "*operations undertaken to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation*" (IAAC, 2000). The US Department of Defense, in 2002, has gone deeper in the definition of IA stating that these measures protect and defend information and IT system by guaranteeing availability, integrity, authentication, confidentiality and non-repudiation.

Thus, information assurance incorporates a holistic approach, including scientific, technical and managerial capabilities, in order to protect and defend information systems. Information assurance includes system and network administration, systems security engineering, information assurance systems, cryptography, threat and vulnerability assessment, risk management, web security, emergency response teams, information assurance training, education,

and management, computer forensics, and defensive information operations. All these aspects are fundamental in ensuring the protection of vital information and data.

Information assurance predisposes five general objectives that should be ensured throughout information life cycle, which is. The first aim is availability which means information must be punctually accessible to authorized users. This variable has three dimensions, space, time and access mode that assess IT system validity and determine importance level of information according to criticality and delivery timing. Integrity assesses the quality of IT system, which reflects its correctness and reliability. It represents strictly protection against non-authorized alterations or damages. Therefore, the integrity of IT system and data ensures that there is the exact match between received and send information, its authenticity and non-alteration. Integrity comprehends also infrastructural components since they have a strong functional interdependency. Integrity can face four threats originated voluntarily or involuntarily; for example, environmental threat is due to involuntary origins, while hardware, software and human threats can be either voluntary or not. Especially the voluntary human threat can generate massive damages to business and that can propagate along the supply chain.

Authentication assesses security and protection actions planned to determine the "*validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information*" (Department of Air Force, 1998). It concerns the identification and verification of user, using restricted access through login and password.

In order to protect information from unauthorized disclosure, confidentiality deals with tutelage and conservation of sensitive data, by limiting the access to authorized and aware users. Thanks to clear authorization system is possible to detect any illegitimate behaviour and violation of confidentiality.

The last objective is non-repudiation which gives "*undeniable proof of participation*" (Hamill *et al*., 2005), since there are attribution documents that prove the occurred information exchange among users. It assesses mainly the transmission system, it uses digital signatures, certified emails and

cryptography, which are tools aimed at ensure warranty and protection of information.

Information assurance is required particularly in certain risky area (The Office of the Assistant Secretary of Defense for Networks and Information Integration, 2009) in which information integrity may be jeopardized. For example, in those areas in which integrity and confidentiality in storage and processing needs greater awareness and protection, IA should be better addressed and employed. Also, the segregation of sensitive information is a key objective of IA strategy. Another point of vulnerability of assurance is the proper configuration of systems aimed at protecting computing platforms from network-based attacks. Moreover, IA should ensure that hardware and software are robust and resilient and that can perpetrate their intended functions.
These are the main challenges to be addressed and to be checked during information assurance strategy in order to ensure clients and users that information and data are properly managed.

Principal characteristics of assurance are the guarantee and cover against loss due to a specified risk or contingency, the confidence retained thanks to verification and the provided freedom of action coming from confidence (The Office of the Assistant Secretary of Defense for Networks and Information Integration, 2009). Alongside with information assurance, there is cyber and identity assurance which complete the protection required by sensitive data.
Cyber assurance comprehends measures aimed at preparing "*net-centric missions*" (The Office of the Assistant Secretary of Defense for Networks and Information Integration, 2009) and information in order to be able to respond to adverse events. It is the justified confidence in networked systems and their security and robustness to efficiently meet operational needs also during attacks or failures (Alberts *et al*., 2009). This level of assurance requires operational security assessment across all aspects starting from acquisition, development and deployment. The best approach to cyber assurance would be to extend dimensions of protection to new borders, addressing multi-program acquisitions and spanning to multiple organizations, in order to reflect the highly interconnection among environments. Consequently, cyber assurance

has to be effectively incorporated into daily operations, not anymore treated like a separated add-on action. Therefore, the integrated decision-making path would link and bind management perspective with specialized technical and operational realities, in order to properly determine and evaluate the impact of decisions at more levels (Alberts *et al*., 2009).

Identity assurance, meanwhile, ensures that integrity and authenticity of identity information and infrastructures are undamaged, while security and privacy are maintained. IAAC's roadmap starts from developing electronic identities and a national identity infrastructure (IAAC, 2008), since there is a wider use of citizen electronic identities which will include significant assurance risks, like reliability and security, that will need to be addressed.

According to EU fundamental rights charter, everyone has the right to the protection of personal data, which must be processed fairly only for specified purposes and on the basis of consent on the basis of law legitimateness (Gonzàlez Fuster, Gutwirth, 2012). It is essential to propose and actuate processes of encryption for any information that clearly or not links identifiable person with sensitive information about them, whose release may cause harm or distress to them (Industry security notice, 2010). Other challenge is allocating responsibility, which is a sensitive topic especially when data breaches take place, as it happened when 25 million of confidential personal data records loss by HMRC in 2007 caused a lack of trust in organizations. UK government was blamed of blindness to the potentiality of bad handling of sensitive data may actually cause (IACC, 2008). However, also private organizations have fluctuating trust rating, for example banks received 66% out of 100% of trust rating, while mail order companies received just 24% (Hallinan *et al*., 2012). It is difficult allocating responsibility for safely handling personal data because public opinions tend to change according to the nature of data collection owner. In fact, according to survey respondents, on social networks individuals should be considered primarily responsible for their personal data and privacy, whilst private companies should be fined if they misused or unprotected personal data (Hallinan *et al*., 2012).

Furthermore, information assurance notion is strictly linked to information security; however, the latter is from computing science, whilst the former is the

result of interdisciplinary and multidisciplinary approach to criminology applied to informatics, developed alongside with digital forensic. They are differentiating also because information security has as objective to find solution to system malfunctions and errors usually generated as accidental events, while information assurance protects primarily systems from voluntary attacks which are aimed to violate security targets.
Information assurance can be expressed as a technical strategy which helps military and civil businesses in the management of massive informative flows, with the primary aim to protect and secure information. Therefore, information assurance aims to protect the quality of information and it is not totally focused on security, which is a dimension of the quality to be ensured.

Information assurance is all the measures undertaken by businesses to manage risks related to use, processing, storage and transmission of information and data, by ensuring availability, integrity, authentication, confidentiality and non-repudiation (Antinori, 2011).
Different models have been developed around these five objectives during the years, improving capabilities and characteristics in order to be better mouldable over next-generation businesses and their retained information. Indeed, the strategies applied by firms are essential to understand the willingness to be exposed to risks, and therefore, for an insurance operator, the risk behind the investment required to cover damages.
Therefore, information assurance represents the first step of risk management strategy in order to employ self-protection against malicious attacks or erroneous use of information and data.

3.2 APPLIED MODELS OF INFORMATION ASSURANCE

Information assurance ensures that information and information systems are available to decision-makers when needed, that data are accurate and complete and that control of these is ensured and maintained (Hamill *et al*, 2005). Moreover, IA should ensure that, even if an accident occurs, detection capabilities, recovering control and restoring IT system exist in order to effectively respond to loss of control that threats integrity of data and information. In this scenario of control loss, it is helpful to take proactive actions in order to set protection measures and put into action defence measures by integrating secure technologies and best practices.
The increasing threats that government, commercial and individual institutions face highlights the need for stable and efficient information assurance, in order to counterattack or at least be prepared for the increased capability to inflict damages to the information systems. The information assurance strategy needs to balance valuable resources, which is time, money and specialized persons, with potential reductions in operational capabilities, due to budget cut or adverse situation.

The original design of the first network on which Internet is based, ARPANET, generates high risks about security and protection, since it has been created with the objective of openness and flexibility, excluding security. These security vulnerabilities have to be faced by governments and businesses, which must deal with unrestricted insiders who can easily retrieve information. Thanks to available and obtainable tools and technology, external and internal threats can capitalize upon IT vulnerabilities or even just take advantage (Hamill *et al*, 2005).

It needs to keep an eye on critical infrastructure protection, therefore it is useful to identify sectors that share common characteristics, and so linked through strong interdependencies, and that rely heavily upon information technology. The sectors which rely mostly on information is banking and finance, energy supply, physical distribution, information and communications and vital human services (President's Commission on Critical Infrastructure Protection, 1997).

Since information systems have a bigger role in operations, in fact IT systems are in charge of controlling, monitoring and sometimes also managing daily operations trough the calculus and elaborating capabilities, this strong interdependence is to be checked in order to assess the status of these critical infrastructures and pushing far risks of alterations, unauthorized access and damage to IT systems.

It has been used a flat approach to risks, since, according to Antinori (2011), regular strategic actions would be prevent, detect and react to accidents and threats. However, nowadays, it is usually preferred a behavioral approach to threats and risks in order to understand better the behavioral patterns of attackers, which makes possible predict the attack and model the best response to intentional and motivated attacks.

Information assurance has been through an evolution that brings to businesses and governments the right tools in order to assess the five main objectives availability, integrity, authentication, confidentiality, and non-repudiation (US Directive 8500.1, 2002).
Now, it is going to be presented the most significant models in IA field which have brought to the new conception of information assurance in modern firms.

3.2.1. CIA TRIAD

The CIA Triad is the first model of information assurance, and therefore it is simple in its characteristics but it is widely-applicable as security model. CIA expresses the threefolding of information attributes and connected to information network and it stands for confidentiality, integrity and availability (Antinori, 2011); these characteristics should be ensured in any secure and protected information system, from user's privacy to encrypted data. Its first objective is to help constructing a security approach in business, in governments and private users towards information and data systems.
Confidentiality aims at protecting sensitive information and data from unauthorized access and disclosure, in fact this characteristics of confidentiality ensures that privacy is maintained and that private information are secured and

inaccessible by unauthorized users (Perrin, 2008). For doing this, it needs to define and enforce proper access protocols and secured protection levels for information, it could be necessary to organize information with diverse security level accesses, according to what kind of damage could provoke if confidentiality was breached (Perrin, 2008). According to Perrin (2008), the most common protocol in order to prevent confidentiality breaches is to include Unix file permissions, organize access control lists and file and volume encryption.

Integrity is mainly referred to data integrity by protecting data from unauthorized alteration or removal and at the same time there is need to ensure and asses changes done by authorized users that can provoke damages, that can be tracked and it is possible to recover data and information (Perrin, 2008). Therefore, it should be maintained and assessed accuracy and consistency of data over the entire life cycle (Boritz, 2011). Despite access should be restricted and protection from changes strict, there are data that should be the most open as possible, such as user file, but in those case it should be ensured the reversibility of the mistake and change (Perrin, 2008).

Last but not least is availability which describes the need to have access to information when needed, so that systems and authentication protocols have to properly work in order to make possible to access available data (Perrin, 2008). In order to improve availability, high availability systems have the necessary architecture oriented at improving availability and decrease the possibility of disruptions. Moreover, these advanced systems can cope with hardware failures, power outages and multiple network connections and deal with denial-of-service attacks (Perrin, 2008), that will be presented in Chapter 4. In order to ensure the highest grade of data availability, high availability systems are advised to be clustered and to plan rapid disaster recovery management (Perrin, 2008).

However, CIA triad model presents limitations and blind spots that need to be addressed by other modified models (Antinori, 2011). In fact, CIA triad is focused entirely on information, leaving behind hardware and what this lack means. This limited view ignores the possibility of physical breaches, by protecting only the software system characteristics; therefore it does not take into account protection plan for unauthorized access to hardware resources.

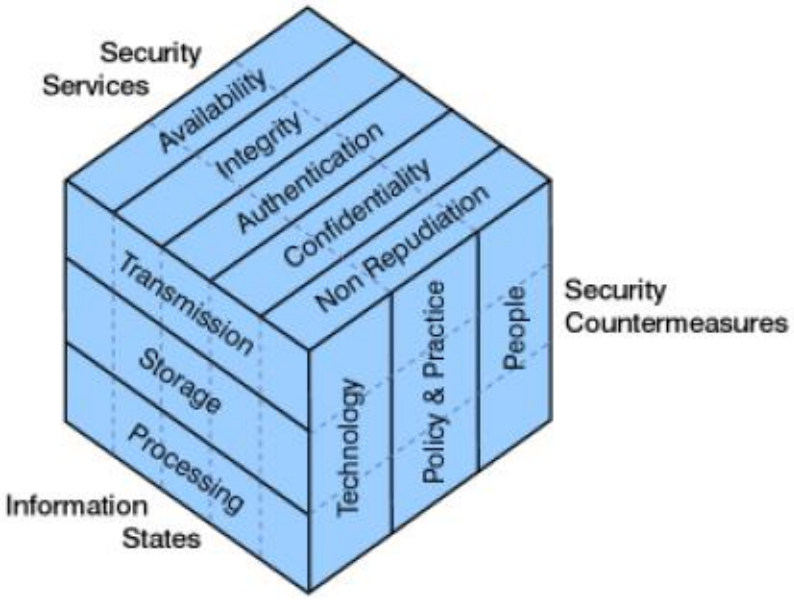
Consequently, if CIA triad model is applied, it needs to be supported by other protection plans and to secure all the points not covered by this simple model.

3.2.2. FIVE PILLARS

A development of CIA triad is five pillar model, ideated by US Department of Defense, it introduces two more characteristics than CIA triad, which is authenticity and non-repudiation. National Information Assurance Glossary (2006), where US Department of Defense introduce first this model, defines information assurance as aimed at defending information systems " *by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation*" (National Information Assurance Glossary, 2006) and restoring and protecting these networks. These two attributes do not refer to information but instead to describe procedures used to assess and protect the three CIA characteristics (Dardick, 2010) (Antinori, 2011).

Authenticity refers to genuine authentication and to the established authority for correct access, usage and storage of information (Dardick, 2010). Whilst, non-repudiation assures that conclusions of analysis are complete and reflect real data and information, therefore they cannot be repudiated (Dardick, 2010). In figure 3.1, it is easy to notice how information assurance, thanks to this model, is spread over the majority of processes of information usage. It integrates countermeasures, acted by technology, practice and people, with stages information goes through, such as processing, storage and transmission, which are controlled and assessed through CIA characteristics plus authenticity and non-repudiation.

Figure 3.1: Five pillars model of Information Assurance



Source: http://www.ibm.com/developerworks/library/s-confnotes/figure1.gif

3.2.3. PARKERIAN HEXAD

The third model is Parkerian hexad, introduced by Donn B. Parker in 1998, and it is influenced by CIA triad model, but it adds three more attributes, authenticity, utility and possession or control, it needs to be noticed that it does not take into account at all five pillar model (Dardick, 2010). These characteristics refer to information attributes, on the contrary of five pillar model. Authenticity, in this model, means genuineness of information as well as of users, who is entitled to access it (Antinori, 2011). Utility is referred to usability and usefulness, that means it is referred to format and support of released information (Antinori, 20011), not to be confused with availability, which is already expressed in CIA attributes. Possession or control is relevant when impairment of information is caused by confidentiality breaches, by subtracting not the information *per se* but instead the container is breached or altered (Antinori, 2011).

In figure 3.2 it is possible to notice the path that information assurance models have been trough, and at the same time, how these three first models, CIA

triad, five pillar and Parkerian hexad, do not reach a complete coverage for information protection.

Therefore, other models have been developed and studied in order to reach the maximum and optimal protection for information and data, in order to ensure their integrity, availability, authenticity and confidentiality, essential characteristics for sensitive information that need to stay so.

Figure 3.2: Fundamental characteristics of CIA triad, Five Pillars and Parkerian Hexad models of IA

CIA	5 Pillars	Hexad	Components
●	●	●	Confidentiality – ensuring that information is accessible only to those authorized to have access
●	●	●	Integrity/Consistency – perceived consistency of actions, values, methods, measures and principle – unchanged "is it true all of the time?" (Verification)
●	●	●	Availability/Timeliness – the degree to which the facts and analysis are available and relevant (valid and verifiable at a specific time)
	●	●	Authenticity / Original – quality of being authentic or of established authority for truth and correctness – "best evidence" (Validity)
	●		Non-Repudiation / Accuracy – transaction cannot be denied (Validity) – no alternate hypothesis
		●	Possession / Control – i.e. chain of custody
		●	Utility/Relevance – "Is it useful? / is it the right information?"
			Completeness – "Is it the whole truth?"

Source: Dardick G.S., Cyber Forensics Assurance, Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

3.2.4. INFORMATION ASSURANCE MATURITY MODEL

In UK, a special para-governmental agency has been formed in order to ensure vital policies on security of communications and electronic data, in partnerships with industry and academic scholars, forming UK National technical authority for Information Assurance.

Alongside with IA assessment framework (IAAF), UK authority for IA created information assurance maturity model (IAMM) to assist and help

businesses at implementing national IA strategy (CESG, 2010). Thankfully to IAAF, it is possible to organizations to conduct self-assessment about the undertaken IA strategy by independently reviewing weaknesses and strengths of IAMM. By benchmarking ongoing information assurance practices and reporting improvements, information risk owners are enabled to establish a comprehensive strategy that can address each weak point in order to make IA stronger, more mature and more reliable (CESG, 2010). The strategy will follow three main characteristics of IA, that is embedding IA culture within the organization, by embedding information assurance within the culture of employees and employers; then it must be implemented best practice IA measures, by undertaking systematic monitoring of IA values and weaknesses; and by ensuring stakeholders that compliance to IA strategy is effective and work effectively (CESG, 2010). By reaching these three goals, IAAM can help increasing trust in information systems and management, spread inside and outside single departments. However, in order to effectively plan IAAM strategy, it is fundamental to undergo systematic and periodic self-assessment supervised by IA review team. A structured routine for self-assessing IA strategy helps IA review team members at spotting and recognizing the most crucial deficiencies that can weaken data protection (CESG, 2013). Self-assessment process and, in general IAMM, requires strict cooperation and partnerships of each department of firm, since they produce documents essential to assess and correct IA strategy in order to effectively response to real environment (CESG, 2013). Therefore, self-assessment required by IAMM is essential "*to provide a rough and ready assessment of the extent to which effective IA risk management processes and procedures are embedded within a Department*" (CESG, 2013).

As it has been showed, IAMM mirrors more a 360° concept of IA, as it needs that IA philosophy is embedded in cultural sphere of workplace, and not anymore a mere process to ensure data integrity. This model requires high level of cooperation of many actors within the company in order to ensure an integral approach to help achieving the desired and established level of maturity.

3.2.5. COMMON ASSURANCE MATURITY MODEL

With the increase of cyber attacks and security exposures, infrastructure protection must be sided by robustness of operational systems and software. Cloud computing, moreover, poses more questions and risks upon system protection and data integrity. Therefore, it requires major attention and care because this technology makes more available and retrievable organizational valuable and sensitive assets in third-party hands, questioning about security, governance and compliance (CAMM, 2011). According to Samani (2010), almost 88% of surveyed customers find security concerns as the key challenge to adopt cloud-based services.

Consequently, a new model approaching these challenges and concerns about cloud computing security seems to be needed by market. Thanks to common assurance maturity model (CAMM), businesses can consistently assess service providers information assurance, can confront IA since CAMM model provisions clear, concise and standardised results, moreover a common model provides a framework supporting transparency and attesting IA maturity of a third party providers and suppliers (CAMM, 2011). In fact, a wider adoption of cloud computing services needs an objective, consistent and complete framework in order to ensure properly information risk management along the supply chain. In this way, cloud service providers can clearly demonstrate their maturity level of information assurance through assessment of governance and data protection and independently auditing providers functions and process (CAMM, 2011).

CAMM has the ability to demonstrate to stakeholders the commitment to privacy and security, improving the general attitude to governance and security, in addition this discriminates suppliers who demonstratively publicise their focus and care about information assurance and data protection from suppliers who do not care or may not take IA seriously (Samani, 2010). Moreover, CAMM can be adapted to any company, from small to large since it is characterized by being modular and scalable in order to meet more and different organizational and operational needs (CAMM, 2011). CAMM provides a single approach for external suppliers assessment by ensuring

standardization, interoperability and portability, which increases the acceptance by numerous and different organizations and existing standards (Samani, 2010) (CAMM, 2011).

CAMM offers numerous advantages to customers and suppliers of cloud computing services, which can make easy the adoption of this model (Common Assurance Maturity Model Steering Committee, 2010). As said, this model provide objective assessment facilitating the comparison among IA maturity of different alternative suppliers influencing in this way important purchasing decision about choosing IT services outsourcing or in-house solutions, if more secure and protected. Adopting CAMM reduces compliance cost and efforts with respect to a greater shared benefits and it increases business agility since customers can attest that suppliers' IA strategy is aligned with risk appetite. Most importantly, CAMM can effectively help businesses to construct a strategy addressing present weaknesses in order to attain higher levels of maturity reassuring clients. CAMM represents a model focusing on risk management rather than merely control ex-post processes. Therefore it focuses on design and implementation of controls, managing confidentiality, integrity and availability of information, which reflect CIA triad model objective.

In conclusion, CAMM provides trustworthiness, which indicates safety, security and reliability of data and information, through supply chain within and across the Internet (Common Assurance Maturity Model Steering Committee, 2010). It completes other models integrating an extended approach and addressing new challenges that business face nowadays, like cloud computing which represents a modern and new business process.

3.3 MANAGING RISKS AND DATA STRATEGICALLY

The models exposed previously deal with handling sensitive information and data, by respecting characteristics which express the integrity and security of these data. Thanks to CIA triad and the more complete Parkerian Hexad, businesses can tangibly assess protection and security toward the processes chain and supply chain of information and data. Moreover, thanks to CAMM, private business can be reassured of the protection level and efforts undertaken by Cloud computing services providers, which handle and store nowadays important share of sensitive data.

However, the increased reliance on IT resources has exposed business to higher risks to be faced and new risks emerge that may be easily exploited. IT risk came out massively in 2000, by being the most significant risk for commercial and industrial businesses (Roberts *et al.*, 2012), while in 70s IT risk was virtually non-existent since firm reliance on technologies and ICT was low and non-significant. Moreover, risks related to IT can emerge, such as malicious interferences, fraud and theft perpetuated through ICT channels (Roberts *et al.*, 2012). These related risks have a larger and more significant impact on business in terms of costs and robustness, since it needs to educate and train staff, to prevent and mitigate negative events posing adequate back-up systems and security controls (Roberts *et al.*, 2012). Also external risks, which are not controllable by organizations, have increased the impact on firms, such as electric blackouts or other critical infrastructures shutdowns.

Therefore, it should be applied a strategic risk management, an iterative process for identifying, assessing and managing all kinds of risks and uncertainties in order to protect activities and data (Frigo, Anderson, 2011) (NISRA, 2011) (UK Government Actuary's Department, 2013). The strategic risk management can help identifying, monitoring and managing the risk profile of the organization which is determined by strategic plans or new strategy (Frigo, Anderson, 2011). Even if a risk taking profile can bring disadvantages and challenges to business, which imply volatile earnings, increased cost of capital and higher exposure to market unpredictable needs (NYU Stern School of Business), there are still positive sides of risks, such as

intimidating competitors, exploiting new and unexpected opportunities, being a dynamic entity which gives to and pretend from businesses flexibility (Roberts *et al*., 2012). The dynamics of risk management widens the action field, as it takes into consideration the complex environment, by analysing numerous opportunities in order to enable the business management to take informed decisions about strategic plans (Roberts *et al*., 2012).

According to CNSSP no. 22 (Committee on National Security Systems, 2012), organizations must put in place organization-wide programs in order to manage and mitigate any information assurance risks which are interwoven in organizational and business operations, and due to individuals' behaviours and to external relationships.

Practically, strategic risk management is the process of identifying, assessing and managing risks and uncertainties, coming from internal or external environment, which could threat operational capabilities of the firm (Frigo, Anderson, 2011). In order to be efficient, it needs a strategic view and approach to risk considering the effects of various scenarios on the overall ability to achieve business goals and objectives, and it requires to be embedded in any strategy plans, as it is a continual process to be run at any organizations layer and unit (Frigo, Anderson, 2011).

Four different risks are analysed by Roberts *et al*.(2012), such as strategic risk, change or project risk, operational risks and unforeseeable risk; meanwhile, two more risks have been discovered to be common and transversal with respect to these four macro risks, which is financial risks and knowledge risk (Roberts *et al*., 2012).

What relates to information assurance is knowledge risk and IT risks (Roberts *et al*., 2012). The latter, IT risks, is part of internal risk that a company may face nowadays due to an internal dependency on ICT, which increases, therefore, the sensitivity to higher likely to CII or critical infrastructure failures. Moreover, IT fraud or cheating is categorized as IT risks, and it could be either internal or external. Other causes of IT risks may be power failure, defective hardware or software, virus infection, lack of back-up and stand- by provision, deficiency of IT support staff, internal malicious damages, intentional or not, and outdated protection systems (Roberts *et al*., 2012). All of

these negative events can create a risk which organizations need to face immediately in order to put into action an effective plan. In fact, the effects of IT risks which have not been correctly addressed could be loss of system records, severe interruption of operational capabilities which can spread to many business units, loss of reputation, disruption of services (Roberts *et al*., 2012). The magnitude of the effects is related to the level of reliance upon IT functions, which is increasing steadily in firms.

Different but related to IT is knowledge risk which expresses information stored using IT, and on which is applied information management and knowledge management and planning (Roberts *et al*., 2012). As IT risk, also knowledge risk is directly proportional to the IT usage level, as the more IT is used within companies, the more companies become exposed to these risks (Roberts *et al*., 2012). It is essentially related to "*not being able to access*" sensitive and "*crucial business information*" (Roberts *et al*., 2012), a coercive disruption of access to information; it differs from IT risks, since it does not involve the information technology per sè, but it's just referred to information and data valuable to businesses. The access can be restricted or denied because of hacking sabotage, malicious interferences and espionage. But, knowledge risk is due also to non-IT reasons, how the loss of key capable persons, especially after a hostile acquisition because of disillusionment or unwillingness to adapt, can demonstrate (Roberts *et al*., 2012) and it is mirrored by possible negative outcomes of the acquisition, such as negative stock performance or massive dismissals and resignation.

Since there is a growing trend to conceive and treat data and information as key assets, a trend duplicated by the higher recourse, handling and collection of information and data, it is highlighted the need of strategically and structured managing information, thanks to information management, which is the collection and management of information. Information meant as strategic resource is the pivotal point of information management, therefore organizations started or are starting now at recognizing the value and the potentialities of information and data if well managed, processed and stored,

whilst realizing that these benefits have to be counterbalanced by costs of applying such an expansive management (Detlor, 2010).
Information management, so, is about the control established over the method and process how information is created or acquired by external sources, organized and stored and distributed in order to enhance better information and responsible decisions. It is an effective tool for promoting and improving information access and competition (Detlor, 2010) (Reponen, 1993), since it improves the quality of decision-making process and, therefore, the decisions themselves.

The actual goal of information management is to help organization to access, process and use information more efficiently, effectively and easily (Detlor, 2010) (Information Management Strategy, 2004). The power of information well managed is tangibly expressed in organizations, since it enables the overall business to "*operate more competitively and strategically*" (Detlor, 2010), moreover, it ensures a better accomplishment of tasks and duties thanks to better and deeper information (Detlor, 2010).
The essential aim of information management is ensuring the right information is accessible by the right and authorised person in the right format and integer at the right time (Alberta service, 2013), all of these characteristics reflect IA models, like CIA triad or the more complete Parkerian Hexad (Antinori, 2011), restoring the connection between information assurance and proper and effective management system of information.

According to Detlor (2010), there are three approaches to information which, in turn, change the approach to manage these assets. The most predominant in business field is the organizational perspective which deals with all-information process management and strict control over the entire lifecycle of information, from creation or acquisition to use and implementation (Choo, 2008), helping reaching competitive and strategic objectives. This approach benefits the organization by reducing costs, thanks to US Government's Paperwork Reduction Act of 1980 by minimizing paperwork burden and the overall costs of supply chain of information; it reduces risks and uncertainties, through an efficient information flow through units; it adds value to existing

services or products and it creates new value to new information-based outputs, by increasing and improving customer buying experience thanks to more shared information.

The second perspective is the library one which indicates a static role of providing information focusing on the management of information collections in order to help ensure clientele of library of accessing and borrowing data and information (Branin, 1990). The library activity has to be surrounded by collection policies development and the construction of a budget, selection processes, moreover, it should be analysed the usage and research entries in order to satisfy end-users needs, staff should be properly trained, preservation policies are needed and it needs to develop external cooperation with other collections and libraries.

The last approach is personal perspective, it refers to "*to how individuals create, acquire, organize, store, distribute and use information for personal purposes*" (Detlor, 2010). It manages every-day information or work-related data, such as calendars, work schedules and project files. Similar to organizational perspective, it differs because it is exclusively related to individual sphere of needs and information.

In order to effectively assure information it is not enough to apply IA models, but organizations have the duty to implement a rounded-approach to risks, in particular to knowledge and IT risks, and to management of information flows.

In general, a standardized information management plan will be able to handle and manage information throughout the lifecycle (Detlor, 2010). At creation level, it should be ensured that data follows normalization rules in order to promote data integrity. If it's acquired, duplicates and accessibility will be the focuses of IA teams in order to make the organization information system agile. Data and information must be protected against unauthorized accesses, and privacy and security need to be ensured, also thanks regular backups. It needs to identify a team of workers responsible for quality (Cumbria Constabulary, 2009) and management of data and information. Mirror copies will be useful in order to not congest or overload networks, moreover old and out-dated information should be archived or deleted in order to keep responsive the overall information system (Baltzan *et al*., 2008).

Information management, in order to be effectively performed and applied to any unit, should develop information strategies, policies and procedures, which give uniformity and clarity to information processes (Information Management Strategy, 2004); moreover, it would be useful to provide managers and employees with best practices and standards functional to every-day operations; an extensive coordination among implemented policies is needed in order to address properly efforts and investments (Information Management Strategy, 2004).

Information management, in conclusion, is focused on the management of the processes that regulates the lifecycle of information and data, from the creation or acquisition to storage, distribution and usage of these key assets (Detlor, 2010). The challenge for information management is about change behavioural patterns and attitudes of users, such as customers and organizations in order to create a significant change and greater focus on how information is used.
The symbiosis of information management practices and IA models would be able to create an efficient internal and external fruition of information, this would make possible to improve operational decisions, including marketing and financing strategies. In fact, information and data are the most valuable assets that organizations can collect, in order to response appropriately to market fluctuations and requests, adapting organization's capabilities and efforts.

Chapter 4

THE IMPACT OF CYBERCRIME ON SECURITY

Chapter four shows the risks that organizations, and general users, meet by using and running IT infrastructures, which represent the pivotal structure for modern organizations. In fact, cyberspace and computer machines are now the key platform in which the complex relation between human factors and economic advantage takes place, as the Internet and its infrastructure connect people, provide governmental services and help running businesses and services. However, the complexities are evident for any users, since risks, threats and vulnerabilities are the first threat to organizational security, and it also represents one of the top threats to national security, second only to terrorism.

In **Multi-angular Perspective about Cybercrime**, it is faced the numerous and various threats and risks that threaten organizations and critical infrastructures. Cybercrime represents a terrible burden for society and economy, it costs billion of dollars for detecting and recovering data and file system, moreover it implies other costs, such as intellectual property losses, due to cyber espionage and cyber attacks perpetrated trough worms and viruses, breach of privacy and financial losses. The dark side of the Internet is going to be analyzed, as it allows to perpetrate attacks and offensive threats thanks to anonymity and smoky environment. Cyber attacks, cyber terrorism and cyber warfare will be defined and analyzed for their consequences on organizations; this distinction is useful in order to plan an efficient and suited security strategy. Cybercrime develops challenges also in geopolitical and legislative issues that need to be addressed and solved with normative and strict law enforcement.

A prospective analysis is conducted in **Significant Examples of the Dark Side of the Net**, in order to conjugate a passive attitude towards incidents and attacks with a proactive approach in order to be ready to deal with severe

cyber-attacks. This section aims at analyzing the most significant and media-famous cyber attacks that struck the Internet and all its users.

Implementing Cyber Security as Deterrence for Cyber Attacks shows the importance of cyber security due to the steady growth of cyber or physical vulnerabilities that could be exploited by cybercrooks. By ensuring security culture, it helps protecting networks and information. By implementing frameworks, it gives managers a valid help and approach in order to construct security strategies. Moreover, there are passive and offensive cyber actions which enable States and always more organizations to counterattack cybercriminals in order to prevent or respond to cyber attacks.

Chapter 4

THE IMPACT OF CYBERCRIME ON SECURITY

4.1 MULTI-ANGULAR PERSPECTIVE ABOUT CYBERCRIME

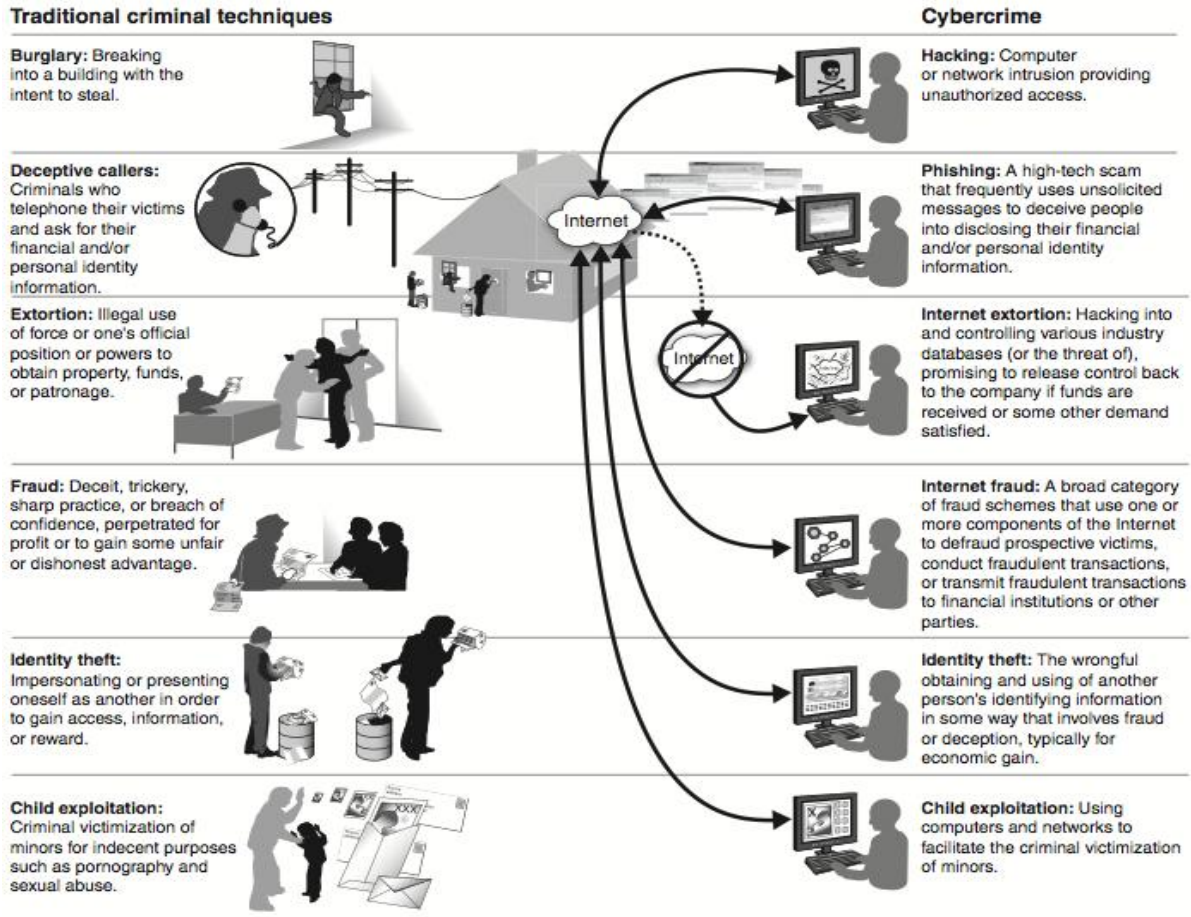
Since ICT represents the pivot of the "*world system*" (Antinori, 2008), cyberspace and computers become the key platform for the complexities of human and economic flows, by running businesses, connecting people and providing government services. As previously mentioned in chapters 1 and 2, Internet and its applications express the global nature of interconnections between critical infrastructures. However, the higher the interconnections and interdependences, the higher the reliance on the Internet which creates opportunities to be exploited by cyber attackers and increases the shock wave and damages caused by the attack. Since the beginning of this architecture, cyberspace had disruptions caused by malicious actors but they lay beyond being just technical or criminal issues (Healey, Grindal, 2013). Cyber conflicts do exist in the overlap "*of national security and cyberspace, where nations and non-state groups use offensive and defensive cyber capabilities to attack, defend, and spy on each other*" (Healey, Grindal, 2013), in order to retrieve political or security information.

Cybercrime is defined by European Commission (2007) according to three different connotations; the first includes traditional forms of crime such as fraud and forgery related specifically to crimes committed over electronic communication networks or information systems. The second meaning is about publication of illegal contents over ICT. The third meaning refers to crime uniquely pursued over electronic networks, such as attacks against information systems, denial of service or hacking. This category is considered to be the most dangerous since these types of attacks can be easily directed also against critical infrastructures, with disastrous consequences for the whole society (European Commission, 2007), intra and extra national borders because of international interdependencies, explained in chapter 2.2. Moreover cybercrime can be committed on a mass-scale and long-range, complicating technical

aspects of investigative methods in order to locate the attackers. Consequently, cybercrime has become a silent global and digital epidemic, whose victims feel powerless against "faceless" cybercriminals (Symantec, 2010). Victimized users are reported to hit nearly two thirds of users around the world, with percentage ranges from 65% (Symantec, 2010) to 69% in 2011 (Norton, 2011). Moreover, the rate of growth and sophistication of these attacks has worried nations and governments and challenged security and defense strategies.

Because of these reasons, cyber attacks are considered by US National Intelligence as the most pressing threat to US security, ahead of Islamist terrorism, although the likelihood of an event is admitted to be very low (Dyer, 2011). The same way as terrorism and other national threats, cybercrime is associated with different and numerous losses, estimated to be approximately at worldwide level US$1 trillion (Ponemon Institute, 2013), and costs derived by enhancing better passive cyber defense and in some cases planning offensive cyber actions. Cybercrime, moreover, is linked to financial losses, intellectual property theft, breach of privacy and other social implications, which make cybercrime comparable to traditional crime techniques, as figure 4.1 shows.

Figure 4.1: Cybercrime as extension of traditional crime techniques



Source: Government Accountability Office

As the majority of users has been infected, computer viruses and malware attacks are the most common and spread threats (Symantec, 2010), especially in New Zealand, Brazil and China where more than 6 computers out of 10 get infected. A silent majority of users has received or been victim of online scams, phishing and hacking of social network profiles and credit card fraud (Symantec, 2010).

According to Prof. LaBrie PhD (Symantec, 2010), users tend to accept cybercrime as they are permeated with learned helplessness, which is a phenomenon that takes place when people do not have enough knowledge of a problem or they do not know how to resolve it, therefore individuals accepts situation although they feel bad or angry for the situation.

Symantec report (2010) highlights that less than 9% of users feel completely safe when surfing the Net. Therefore, a major challenge is the resolution of damages caused by attacks, which erodes time and money. On average, it takes four weeks and US$ 334 to resolve an average cybercrime incident (Symantec,

2010). However, it changes around the world in time and expenditures, as shown clearly in figure 4.2, which triggers the emotional baggage of stress, anger, embarrassment and loss of irreplaceable data of sentimental value (Symantec, 2010).

Figure 4.2: Differences in time and money expenditures for resolving cybercrime incidents

Source: Cybercrime Report: The Human Impact, Symantec, 2010

Attackers calibrate their strike, in order to maximize infection propagation and effects, according to users buying and entertaining preferences, as it shows a 40% increase in websites delivering infected MP3 files or built in order to spread the infection (McAfee report, 2010). The spread of infections is due also to unsecured Wi-Fi hotspots and the growth of websites and services sensitive to private information, such as iPod and iTunes and Napster (McAfee report, 2010), increasing customer data breaches into large companies databases. Nowadays, identity theft becomes an issue that need to be properly addressed, since this problem affects around 11 million of Americans and many others (McAfee report, 2010).

Moreover, cybercrime shows a globalization trend which redefines the power and players' roles in international relations and politics. This trend changes cybercrime characteristics, as gangs become more discrete but at the same time more experienced; the discretion helps for the timing of exploit unknown vulnerabilities before organizations can patch them.
The equality professed by the Internet makes companies and organization likely vulnerable to malware and cyber attacks (Cisco, 2013). On the contrary, largest businesses with more than 25000 employees have more than 2.5 times the risk of contracting malware with respect to smaller companies. This trend can be explained as bigger enterprises retain higher and more valuable intellectual properties and collect greater amount of consumers' data.

However, cybercrime is characterized by subtle reasons, different from traditional criminals. The most likely reasons for cyber attackers to strike a target is for exploiting three outcome effects, one may be fear factor, which is aimed at creating the maximum fear in people by striking IT installations and especially critical infrastructures. Or attackers try to reach a spectacular factor, expressed in massive direct losses or in colossal media coverage, which makes the actual damage insignificant for cybercrooks. Or because attackers want to exploit vulnerability factors, through which demonstrate the weakness of organizations by causing denial of service or by vandalizing organizations' web pages.
On the other hand, two main drivers can be identified for cybercrime, which may incentivize cybercriminal activities unless an efficient and effective law enforcement does not maintain trust, security and protection of ICT and critical information infrastructures (Càrdenas *et al*., 2010). The first driver is the increasing of potential gains from perpetrating cyber attacks, which increases along with the importance and usage of the Internet. The second is that cybercrime has low expected costs, such as penalties and the possibility of being prosecuted, decreeing computer-mediated crimes more convenient and economically profitable and less risky than traditional crime activities.

Cybercrime is facilitated by the intrinsic nature of the Internet, which is characterized by anonymity, large number law and free valuable contents. In

fact, due to anonymity, cybercrooks can easily hide their identity behind pseudonyms, fake email account and other means (Kim *et al.,* 2013). However, this capability of hiding the true identity has as the result to bring out the bad behaviors of people, who feel legitimated to attack or denigrate other users or take advantage of copyrighted contents. Secondly, cybercrooks tend to hide and retrieve strength from the large numbers of Internet users, which makes impossible for authorities to enforce any copyright law (Kim *et al.,* 2013). This, however, encourages users to illegally benefit of protected material. In fact, the large availability of highly valuable free contents, software, storage services and social media sharing have led users think that any contents and services is free and ready to be downloaded (Kim *et al.,* 2013), this thinking brings to a mass violation of copyright laws, with severe economic consequences.

Cybercrime has well-defined preferences in its targets, which have to meet some criteria in order to reach cybercrooks' aims. In a model ideated by Kshetri (2005), it appears that targets have common traits related to targets' characteristics and likelihood of attacks. In fact, the model shows that if a target has a strong and symbolic meaning and criticalness, the likelihood of being a target and victim of cybercrime is increased. At the same way, the degree of digitalization, which expresses the reliance of organization on networks and ICTs, increases the possibilities of attacks. In fact, it is evident that cybercrooks prefer to attack and direct their efforts to large companies rather than small or medium enterprises (Riptech, 2002). Moreover, organizations are likely to be attacked if they have a high dependence on digital technologies and if their business plans are based on e-commerce, such as online casinos, banks and financial institutions. The state of defense if manifest weaknesses or vulnerabilities are positively dependent on the possibilities of being cybercrime target (Kshetri, 2005).

The magnitude and impact of cybercrime is challenging to quantify, since cyber attacks are not always detected or reported to authorities (Càrdenas *et al*., 2010), moreover there is no standard method for cost measurement in relation with the analysis of likelihood of cybercrime. Furthermore, the reluctance of organizations to disclose information on security breaches is explained because

of the negative impact (Càrdenas *et al*., 2010) that this news causes to businesses, such as a negative financial market impact due to security breach announcement of organization, now perceived more risky; then there are reputation and brand damages, which generate confidence loss in costumers; litigation concerns disadvantage a complete disclosure of security breaches, as investors or other stakeholder may seek through law enforcement recovery of damages; moreover, disclosing may highlight a no-accomplishment of managers to regulations, therefore arising liability concerns; reporting signals to other potential attackers that information systems of organization is vulnerable and easily exploitable; moreover, IT personnel may act egoistically and fear for their job security trying to hide the breach.

Furthermore, organizations act simply as egoistic individuals who care only about their own profit and benefits, so security breaches cost more to society and security projects must be undertaken, with all their economic burdens, by single actors. In fact, the costs of disclosing tend to be significant, as seen earlier, while the benefits, like more efficacy and lower expenditures in security, come slowly in medium, long run, while, at the same time, it benefits the entire market. This creates an enormous gap between costs sustained by just one firm and benefits for everyone, creating a market failure full of free-riding concerns. Losses are composed of direct and indirect costs, including financial losses, also due to theft of money, the estimation of intellectual property costs and losses because of theft or impropriate divulgation, recovery costs of repairing or replacing damages in networks, and intangible losses derived from lack of confidence and trust in the organization (US Government Accountability Office, 2007).

A reliable estimation of economic costs are collected by Internet Crime Complaint Center (IC3), which highlighted in 2008 a sensible increase in complaints, with a growth of 33% over 2007, and a total loss due to online fraud for US$ 265million, that was $25 million more than the previous year (Càrdenas *et al*., 2010), and identity theft is estimated to produce losses for $49.3 billion in 2006 while due to phishing losses are around $1 billion annually (US Government Accountability Office, 2007). Since these estimates do not represent the real value of cybercrime, due to missing disclosure of

security breaches or other criminal activities, the quantification makes clear which big and important part plays cyberspace and its protection for users in general and for organizations and businesses in particular.

In order to give a better understanding of the importance of cyberspace, three major aspects of cybercrime are going to be defined and examined: cyber-attacks, cyber terrorism and cyber warfare. These aspects represent the evolution of cybercrime, which comes alongside with technology advancements, and reflect the different intentions of attackers.
Moreover, a clear and net distinction between these terms is useful when a strategy for security and protection need to be designed, and it needs to take into account the different consequences and targets. In fact, protection has to be tailored in order to respond actively to different characteristics of these cyber threats that change in outcome factors, among fear, spectacular or vulnerability factors, which reflect the intention of cybercrooks, and characteristics that differ in final damages, that could be physical, psychological or financial.

4.1.1 THE DARK SIDE - CYBER ATTACKS

In cybercrime scenario, cyber attacks are the most diffused and dangerous for any user that approach the Internet, as they are conducted world-wide and on a daily basis by targeting individual users, organizations and also government (Orrey, 2011). Cybercrooks use wide and varied attack vectors, in order to exploit the maximum number of vulnerabilities of nowadays-wide offer of applications, protocols and operating systems. Usually, normal users do not even realize that they are targeted by hackers, instead large corporations and governments try to mitigate them, as they are always on alert for cyber attacks.
According to Tatum (2010), cyber attacks are described as "*an attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission*", therefore they represent a real threat and menace to the overall network, as it may be damaged to the point of not performing at all. The motive that lays behind these attacks are normally found in monetary gain, or are politically

motivated or done to gain increasing credibility among other hackers (Orrey, 2011). Therefore, cyber-attacks are considered as a real increasing problem influenced by other factors, like cultural changes, which are reflected in a growing interconnectivity among people, which increases the attackable basis. In fact, the growing recurring to non-traditional work arrangements, but now conducted outside organization's IT network, makes vulnerable to attacks networks previously inaccessible (Orrey, 2011), because of limited external connectivity.

Therefore, organizations have to maintain an adequate level of awareness in order to decrease the likelihood of important damages for the business through education and pragmatic advices for employees at any level (Orrey, 2011). Awareness and education integrated with existing mechanism of protection, such as hardware and software firewalls, pose challenges to cybercrooks as their attempts could be more easily detected in order to start defensive operations. However, awareness and training programs tend to last more than one year, and their benefits can be tangible only in the medium long run, in order to reach a large adoption and a deeper penetration.

Cybercrooks and threat sources are numerous and various, and each category has its own goals, motives, capabilities and funding (CESG, 2009). There could be insiders, *i.e.* disaffected or dishonest employees, hackers, investigative journalists, commercial competitors, organized criminal groups. These categories represent the players in cyber-attacks who damage economic and physical and psychological sphere of human beings. In fact, damages can be a loss of money or under the form of defamation and invasion of privacy and also they can physically harm. These negative aspects are worsening by loss of time and mental repercussions, such as anguish and irritation (Kim *et al*., 2011).

During studies, it has shown how users tend to be vulnerable mainly in three areas, which are network, physical and personal security (Orrey, 2011). These vulnerable areas are the main doors for cyber attacks which propagate in different ways depending on the chosen main door.

Network-based attacks include all those attacks designed to exploit software vulnerabilities at local or remote range or while routing data. However, the growing use of Virtual Private Networks (VPNs) can provide the right level of trust and assurance, but, unfortunately, not every users use these connections, leaving exposed points in the infrastructure (Orrey, 2011). On the contrary there are cloud services, which are now provided by many providers; these services are commonly assumed to be safe and protected, where it is recommended to store sensitive data and information. However, this assumption tends to lead users to a feeling of security even if they are not aware of security programs and protection strategies applied by the providers, and they continue to store data, leaving room to cybercrooks to access them and retrieve important information (Orrey, 2011).

Network traffic has been abused in many ways resulting in high profile incidents, and it can be abused also if Tor network is applied. Tor network ensure anonymity in using the Internet, through an encrypted path or virtual circuit made of Tor routers and proxies, its use is predominantly recommended when free speech and thinking is hampered by governments through filtering and suppression, as it happens in China and Iran. However, Tor network too can receive numerous attacks, threatening the anonymity. The main access to Tor is to set up a Rogue router, which, by benefiting from Tor architecture, modifies an exit node in order to strip off encryption codes piled up at each layer the message goes through, at this point the message is clearly readable (Orrey, 2011). Thanks to Rogue routers, other cyber attacks can be launched, such as sniffing attacks, MiTM, session hijacking and software update services (SUS) (Orrey, 2011). By using sniffing and harvesting programs, Rogue router operator can collect an impressive number of plain-text of Hypertext Transport Protocol (HTTP), and logins credential (Wired, 2007). MiTM, *i.e.* man in the middle, is an attack aimed at stealing sensitive data and passwords by routing victim traffic and passing on the targeted cyber destination. It can be perpetrated through the use of nodes targeting Tor ones, the first is session hijacking, and the second is SUS. Session hijacking simply steals already authenticated connection by stealing credentials or thanks to cookies. Circumventing and modifying SUS works on automatic software update services, which remind user updates and patches to be downloaded. They run

constantly in the background of operating system programs. However, these background programs are easily exploited by attackers, as they represent security open doors, in this way cybercrooks have an opportunity to catch victim's data and control over the machine by using SUS (Orrey, 2011).

Another vulnerable area is physical security, which encompasses tailored attacks by using hardware in order to exploit any vulnerability or weakness in the victim's system (Orrey, 2011), by transforming him in an unsuspecting expander of the attack because of his naivety. Attacks are perpetrated through USB device infected by viruses and malicious codes by eroding autorun or autoplay mechanisms (Anderson, 2010). One kind of attack is USB dumper, which creates background process and, once USB is plugged in, it starts to copy contents in a newly created directory; in this way, the attacker can read and have access to documents and contents at a later time (Orrey, 2011). Instead, USB based viruses and malicious codes use autorun and autoplay mechanisms, through which it infects the system and consequently any USB devices plugged in afterwards, and it creates custom autorun files on USB that will execute them when it is plugged into other systems and machines.

Personal security issues represent open door for attacks aimed at exploiting weaknesses, foibles and naivety of users by constructing social engineering models (Orrey, 2011). Thanks to neuro-linguistic programming, attackers can outline a behavioral pattern, and use different social engineering techniques by manipulating people in order to bypass security measures and obtain confidential information or gain illegal access to them.
In this category, there are many different kind of attacks that can be perpetrated. According to Kim *et al.* (2011), this dark side of the Internet can be divided into two main categories in which the most used cyber attacks are grouped. This taxonomy is focused on technology-centric and non-technology-centric threats, which both put in danger the security of users (Kim *et al.*, 2011).

Figure 4.3: Taxonomy of dark-side Internet

Technology-centric	Spam Malware Hacking Denial of service attacks Phishing Click fraud Violation of digital property rights
Non-technology-centric	Online theft Online scams and frauds Physical harm Cyber bullying Spreading false or private information Illegal online gambling Aiding crime Other reprehensible behaviors

Source : Kim W., Jeong O., Kim C., So J., The dark side of the Internet: Attacks, costs and responses, Information Systems, Volume 36, Issue 3, Pages 675–705, Special Issue on WISE 2009 - Web Information Systems Engineering, May 2011

As shown in figure 4.3, it is clear the distinction between these two cyber categories, therefore, technology-centric elements require technologies and technical skills "*beyond the main-stream Internet technology that most people use for their daily work and life"* (Kim *et al.*, 2011), which include for instance email-harvesting software, capabilities to create and propagate malware, techniques to hack computer systems. It includes spamming, malware, hacking, denial of service (DoS) attacks, pretexting, phishing, click fraud and violation of digital property rights (Kim *et al.*, 2011) (Orrey, 2011).

Spamming is referred to unwanted notices coming through email, and that are mostly for marketing purposes (Kim *et al.*, 2011). They represent a plague that strikes thousands of users, which are bombed with almost 200 billion spam messages a day (Kramer, 2010). Pretexting aims at constructing trust towards the attacker in order to more easily have access to sensitive information, by using prepared scenario and pretending to be IT support staff (Orrey, 2011). Malware is a general term which includes viruses, worms, Trojan horses, spyware and adware. Viruses are contained into program files or hard disk boot record and spread from infected system to others. A worm, instead, is a standalone computer program that replicates itself and propagates across a network by relying on security and protection failures on the targeted computer; unlike viruses, worms do not need to be attached to an existing

program and their final objective is to at least harm the network by consuming bandwidth, instead of viruses, which target to corrupt or modify files (USCB Science Line). Trojan horse looks like a legitimate program but, thanks to malicious codes, it carries out determined actions by causing data theft or loss and possible system damages. Moreover, spyware collects and sends copied data, such as financial, personal data or passwords. By gathering information, it sends these to the attacker without users' permission or knowledge. Adware is an advertising supported software which generates revenue for its author; it automatically displays advertisement, it can be used in order to analyze the preferences of users on the Internet and to advise pertinent goods and services in accordance with individual preferences.

Phishing is a technique to retrieve sensitive information by making users trust look-like authorities websites, such as banks, credit card companies and popular social websites, who enter passwords, credit card numbers and other personal details. The author can resold or use these information for other cybercrime, such as identity theft and fraud (Kim *et al*., 2011).

Hacking, instead, refers to the act of breaking into others' computers thanks to the strong and wide interconnectivity offered by today Internet. However, hacking has different aims, there are white hat hackers, or ethical hackers, who test organizations' network in order to highlight weaknesses and vulnerabilities that may be exploited in a harmful way (Caldwell, 2011), or otherwise, they represent the authors of significant disruption and damages to information systems all around the world (Furnell, Warren, 1999). Other hackers have fun by showing off their technical capabilities. In general terms, they tend to gain access to or destroy sensitive data, or stealing money and digital properties, sometimes causing a system breakdown (Kim *et al*., 2011).

DoS attacks overload targeted computer system with bogus requests in order to make impossible to provide normal services to users. Perpetrators of this type of attack target sites and services hosted on high-profile servers. This threat is common in business, perpetrated by competitors. A different kind of attack is the distributed denial of services (DDoS) which is sent by two or more persons or botnet, which are Internet-connected programs charged of performing tasks, which range from controlling legal channels to send spam or participating in

DDoS. DDoS can be performed also with permission of users, as it happens for Anonymous group's attacks.
Violation of digital copyright is done by posting without authorization digital properties, such as music, movies, books and software. It can be, sometime, indirect violation if properties are posted in file-sharing sites, however, US government enacted in 1998 Digital Millennium Copyright Act which exacerbates fines for copyright violation on the Internet (Kim *et al*., 2011).

In the taxonomy, any other elements of dark nature are considered non-technology-centric (Kim *et al*., 2011).
It is characterized by requiring an offline counterpart, who decide the target in order to orchestrate the crime, which is composed of "*online theft, online scams and frauds, physical harm to people, defamation and invasion of privacy by spreading false or private information, illegal online gambling, aiding crimes, and general reprehensible behaviours*" (Kim *et al*., 2011) and quid pro quo technique (Orrey, 2011). These methods require a deeper knowledge of human behaviour and habits and the authors tend to be more criminal who take advantage of cyber world and its benefits.
For instance, online theft comes afterwards data theft, which is committed through cyber means, like electronic tools, such as wire tapping, packet sniffing or rummaging through trashcan or using hacking, phishing or malware attacks (Orrey, 2011). This crime is perpetrated for financial gains, by withdrawing bank accounts, or for facilitating traditional crimes.
Online scams and frauds require confidence games and naivety of users, who believe in receiving money or property by giving up real money or valuable property. A particular scam is quid pro quo, this technique works as an exchange. The attacker in exchange of something, such as free chocolate at Infosec conference (BBC, 2004), asks for passwords and credentials (Orrey, 2011). Internet can have also physical effects and damages to users, like the case of pro-suicide and pro-ana website by encouraging sensitive users to unhealthy or, worse, mortal behaviours (Kim *et al*., 2011). Moreover, Internet can be easily used for connecting paedophiles with sex victims, or it can represent the mean for cyber bullying, which hurts or embarrasses persons by sending or posting text or images. Cyber bullying causes severe psychological

damages, such as lower and damaged self-confidence and self-esteem, depression, fear and reluctance to participate in group activities (Kim *et al*., 2011). In fact, Internet power to amplify opportunities and range of defamation and invasion of privacy is a threat for individuals and organizations, due also to the global reach and speed of information dissemination. Internet can be considered as an aiding tool for crime, because users post "how to" tutorials helping criminals to break the law, such as helping making explosives, drugs, hacking, spamming and breaking into homes and buildings (Kim *et al*., 2011). Other dark side of Internet is enabling online gambling, which becomes US$29.3 billion business in 2010 (Pfanner, 2010).

Nowadays, attacks are usually carried in combination of more than one technology-centric attack in order to reach the maximum point of damages. Attackers combine characteristics of viruses, worms, malicious codes and other techniques and launch these blended threats against server and Internet vulnerabilities in order to transmit and propagate attacks (Orrey, 2011). Thanks to numerous techniques and strengths, it is ensured a rapid spread of damages and breakdowns and it increases the success of attack.

Another problem that strikes especially organizations is cyber-espionage, which is about extracting value from computers of organizations and governments (Centre for Strategic and International Studies, 2013). Companies have a tendency to underestimate this risk and its costs and consequences; therefore, a large number of businesses are exposed to this threat. The underestimation of damages due to espionage makes the companies feel comfortable, since they believe that espionage is "*part of the cost of doing business in the world's fastest growing markets, and that they can run faster*" (Centre for Strategic and International Studies, 2013).

However, this threat of cyber espionage is a trend expected to rise and grow over years, as it is difficult to detect and stealing vital information is extremely cost-effective (Everett, 2009). In fact, e-espionage is all about costs, "*about information and it's all up for sale somewhere, so the better the data the more money you can make*" (Everett, 2009). Costs lays especially on companies' shoulders, as they lose strategic advantage, intellectual property, customer lists,

competitive analyses and sales data. In 2011, cost of cyber espionage are estimated around $100 billion in losses, which is translated into 500 thousands of job places, as a side effect of cyber espionage (Centre for Strategic and International Studies, 2013). However, cyber espionage and data theft tend to have an internal source, rather than external, nonetheless, it is not less damaging; it may happen by accident, for personal gain, because of discontent, or due to ideological reasons or for blackmailing (Centre for Strategic and International Studies, 2013).

The increased ability of cybercrooks is reflected in their sophistication of attacks and vectors of threats, by duplicating websites and stealing credentials. Therefore, it is essential for protecting individual users and organizations, which are seriously threatened and damaged by cyber attacks, to construct an efficient cyber security.

4.1.2. THE DARK SIDE – CYBER TERRORISM

Even if cyber terrorism term began to be used in 1980s, international focus started in 2000s due to terrible and always more frequent terroristic attacks, there cyber terrorism became a strong potentiality of attacks. America, after 09/11, had fear of possible large attack to sabotage critical infrastructures through computers and cyber space. In 1996, the term was coined in order to properly express "*premeditated, politically motivated attacks by sub national groups or clandestine agents or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets"* (Colarik, Janzewski, 2008). FBI gives a rounded definition, by emphasizing the force and violence of these attacks; it does identify cyber terrorism's goals in intimidating or coercing governments, population in order to achieve the group's political or social aims (Hinde, 1998). In fact, the powerful weapon, alongside with worms, Trojans, viruses, DoS and unauthorized intrusions, is triggering fear and damages to the larger number of people.

Moreover, in support of these definitions, studies discover a strong correlation between political and military conflicts and the frequency of cyber terrorism

events, as it happened during Israel-Palestine conflict and India-Pakistan (Hinde, 1998). These findings support the idea that cyber terrorism reflects a political and military agenda in line with national or predominant group, vision.

Terrorism exploits the benefits of technology and Internet, which are numerous and cost-efficient (Caudle, 2010). Since terroristic groups tend to have limited resource, both financial and sometimes technical, the use of cyber attacks, and sometime hiring professional cyber attackers (Wilson, 2008), respond properly to their objectives and budgeting. Numerous advantages bring terrorism to cyber space, in fact, it ensures lower costs than traditional and kinetic attacks, the actions run in the cyberspace are difficulty tracked, Internet provides anonymity and no geolocation, and it enables the group to attacks anywhere in the world at a safe distance, and hit more targets and affects a larger number of people (Wilsker). These incentives provide to terrorists the ability and capacity of conducting acts of intimidation, coercion and violent extremism through the vast possibilities of the Internet (Caudle, 2010).
Unlike cyber attackers, cyber terrorism is different in motivational purposes. In fact, for skills and techniques, cyber terrorism looks like a cyber-attack, since both groups aim at the breaching systems' security (Furnell, Warren, 1999). However, cyber terrorists act for specific and determined political and ideological agenda, making their efforts and targets focused and specific in order to achieve the objectives (Furnell, Warren, 1999).

Therefore, the effect of act of cyber terrorism may destroy country's economy by attacking critical and vital infrastructures, such as electric power supply and water system. According to Lewis (2002), the next step for cyber terrorists would be large-scale and well-coordinated cyber attacks against national system and critical infrastructures, preferring attacking electrical grids, financial nodes, transportation systems and, due to its growing importance, telecommunication networks in order to coerce or intimidate or even terrorize governments and populations. Some attacks would have terrible effects, such as changing in deadly drugs by accessing drug manufacturer formulas (Wehde, 1998), or by accessing hospital records and changing or erasing medical

information (Gengler, 1999), or by reporting stolen information to best buyers (Desouza, Hensgen, 2003), or manipulating perception and opinion to masses (Stanton, 2002).

Consequently, organizations and business which rely heavily on critical infrastructures may be hit more seriously as they are more vulnerable, detecting "*a massive electronic Achilles' heel*" (Lewis, 2002) in this strong dependency. As critical infrastructures are vulnerable to external attacks, cyber terrorism can effectively influence national security programs' outcome. In fact, cyber terrorism tends to combine physical and cyber attacks in order to maximize their efforts (Hua, Bapna, 2013).

Therefore, the interdependencies require major security and protection especially at technological level, which is particularly vulnerable to many cyber threats and risks.

4.1.3. THE DARK SIDE – CYBER WARFARE

As the Internet opened multiple possibilities of beneficial outcomes, such as educational benefits, more freedom of speech and larger possibilities of forming personal opinions and of communicating with others, however, as it has been shown, Internet hides great dangers and future threats. One of these is cyber warfare and a possible cyber Cold war (Dipert, 2010). It is defined as the next-generation war, as it is a "*strategic war of Information era*" (Aviation Week and Space Technology, 2012), a considerable branch if information war (Kapto, 2013), a development and evolution of warfare since nuclear weapons (Dipert, 2010), a better and more accurate nomenclature is information and infrastructure operations (I2O), however it is commonly indicated as cyber war (Miller, 2012).

Cyber warfare has a broad definition, which says that it is about planned attacks to nations' governmental or civilian systems or their agents against information and computer systems, computer programs, and data that results in enemy loss (Dipert, 2010). It is constituted by conducting military operations by virtual means through cyberspace (Hildreth, 2001) in order to achieve those objectives common to conventional wars, such as gaining political or territorial

advantages or preventing other nations to gain them (Brenner, 2006). Cyber warfare is made of intentional cyber harm caused by agents who impair or degrade through cyber attacks other political or military organizations (Dipert, 2010).

However, cyber war is not completely independent from kinetic war, but it is part of the overall tactic (Kapto, 2013). Even if cyber-attacks capabilities are not fully deployed and not considered the principal weapons by nations, an integrated use of cyber war and kinetic war resulted in optimal offensive and defensive tactics. In fact, cybernetic weapons cannot produce the same damage as conventional war, therefore, from jurisdictional point of view, it is difficult to consider and qualify these cyber attacks as war acts (Report McAfee, 2009).

However, cyber warfare shows growing trends in importance and use in nations' arsenals, as it presents and offers numerous advantages with respect to kinetic war, financial, ethical and operational benefits. In fact, cyber war requires lower costs than developing and maintains troops. Costs for cyber warfare include training and wages of cyberwarriors and investments in hardware and software, indispensable for launching and countering cyber attacks (Brenner, Clarke, 2010). A significant reasoning behind the success of cyber acts is the relative preservation of human and non-human with respect to invasive kinetic war. However, this same benefit is counterproductive since nations are less discouraged in launching cyber offensive attacks (Brenner, Clarke, 2010). This kind of virtual war would preserve warriors from physical injuries, thanks to the possibility of launching attacks in remoteness ensured by cyberspace ubiquity. Another great benefit of using cyberspace for attacks is disguising attacks source, thereby it is essential to avoid responsibility and involvement, and possible retaliation and counterattacks (Brenner, Clarke, 2010).

Here, attribution problem is the greatest challenge to be addressed also for the application of law applied to cyber activities (Huntley, 2010). Attribution problem (Grauman, 2012) (Brenner, 2009) refers to difficulties in establishing the identity and location of attack perpetrators, it is due to Internet designed in order to ensure anonymity and net neutrality. However, there are two main methods to overcome the identification made through IP addresses; the former

is IP spoofing whilst the latter is zombie computers. IP spoofing permits to conceal attackers identity by changing IP address; similar in intention but through different technique is the use of zombie computers, which exploit man-in-the-middle approach (Miller, 2012) by taking advantage of compromised machines and networks of unaware third person in order to conceal and mystify the origins and motivation of attacks. Therefore, traditional Cold war deterrence approaches of retaliation cannot be applied in cyber attacks as it is difficult and time consuming to identify attackers (Miller, 2012).

The use of equal tools and means shared by cyber terrorist, cyber attackers and cyber warriors makes difficult a net distinction; however, it is possible trait a line of distinction thanks to their different intentions and different targets. Cyber warfare has a well-defined target which is attacked during or before the kinetic war or invasion. This kind of offensive/defensive approach, by using cyberspace, is establishing in many countries, according to 2007 FBI report (Markoff, 2010), 108 countries have this capabilities, in which the most offensive countries resulted USA, China, Russia, Israel and France, as shown in Figure 4.4.

Figure 4.4: Diffusion of cyber weapons

Source: Report McAfee 2009 sulla criminologia virtuale- L'era della guerra informatica è alle porte, 2009.

Growing number of attacks with political motivations has a strong impact on international relationships between nations, which are encouraged and incentivised to have access to this new form of war (McAfee report, 2009). This international tension, however, makes evident the vacuum in policies and legislation about cyber offenses (Dipert, 2010). Without an informed and open debate able to construct an efficient law enforcement, it is reminded traditional law theories about warfare, divided in *ius ad bellum* and *ius in bello* (Dipert, 2010). *Ius ad bellum* regards the timing of an attack, *i.e.* when a nation may be obliged to take part in war; it is decided according to different criteria (Dipert, 2010), that are just cause, last resort, the likelihood of success, proportionality, proper authority and right intention. By analysing these criteria, a state should be able to properly make decision, since it is informed and aware of its war decision.

Instead, *ius in bello* enters into force when the war begins and it serves as guideline for morality, ethics and actions in war.

While waiting a proper law, cyber war goes on through skirmishes between major potencies, meaning through aggressive Internet "*probing of military and industrial secrets*" (Dipert, 2010), such as DoS attacks, viruses, corruption of data.

The most probable targets of skirmishes and actual attacks are critical infrastructures, such as financial and banking sectors, electric power, water supply, telecommunications networks. "*Critical infrastructure owners . . . report that their networks and control systems are under repeated cyber attack . . . from . . . foreign nation-states"* (Baker *et al*., 2009), the situation is worsened because critical infrastructures are mostly privately owned, and therefore more exposed to risks and attacks. Many owners of critical infrastructures rely on government help if a cyber attack would occur, however "*45 percent believed their governments were either 'not very' or 'not at all' capable of preventing and deterring cyber attacks"* (Baker *et al*., 2009). Therefore, it suggests that protection and cyber security would be on the shoulders of private organizations that would always be in cooperation with government in order to align efforts and investments.

In fact, the first target in a cyber war would be critical infrastructures which are supported and controlled over networks or the Internet, in order to have the maximum effect with less efforts and costs (McAfee report, 2009). Because of the growing importance of computer systems in running critical infrastructures as control systems (Miller, 2012), these cyber systems are always more used as attacks vectors, therefore SCADA systems, which are the most used and employed in Europe, are the easiest way of access to strike nation's defense and autonomy (Miller, 2012). SCADA has been though technology development in the last years, as it was characterized by remote and proprietary systems and now it is structured as an open architecture which ensures a higher level of interconnection with other critical infrastructures and the Internet (Pauna, Moulinos, 2013b). This passage has had as a result the increasing in vulnerable points in SCADA systems that can be access by outside attackers, so it is essential to secure SCADA though the prompt application of patches in order to solve vulnerabilities and decrease risks of attacks (Pauna, Moulinos, 2013b). Patches can mitigate software flaws, add new features, improve the functionalities of software and firmware in order to reduce the likelihood of malicious attacks. However, they can also represent a risk and their application my represent a serious problem of window of exposure to attacks. In fact, patches may indirectly affect the behavior and functioning of critical infrastructures and SCADA system itself, and moreover, from the release of patch and the actual employing, the system is left unprotected to possible attacks (Pauna, Moulinos, 2013b).

In order to attack, though, SCADA system, it is required a careful planning and preparation (McAfee report, 2009) (Miller, 2012), since attacking SCADA is a complex maneuver which requires capabilities and competencies, efforts that can be made by potent nations that can pay and ensure the best hackers (Miller, 2012) (McAfee report, 2009).

Critical infrastructure attacks can be coupled and intensified with information operations (Miller, 2012). These added operations are designed and projected for disrupting, demoralizing and confusing the attacked nation, in order to ease and magnify the effects of cyber attacks to critical infrastructures and to weaken further nation's defenses, authority and tactical advantage (Miller, 2012). Since there is a first strike advantage, difficulties in identifying and

attributing attacks to offender, a possible defensive action is to pre-empt and prevent "*an expected attack before one's own capabilities are eroded, and to carry out the equivalent of launch-on-warning counter operations*" (Miller, 2012), through retaliation attacks to be carried in cyber space, as also through physical attacks, as America declares that cyber attacks to US may lead to military retaliation using also non-cyber weapons.

Therefore, cyber warfare is delineated as unpredictable and destructive for all nations, as from a cyber attacks experienced as an act of war can result a defensive/offensive action through invasions, kinetic episodes of war, spiraling out of control the entire situation (Miller, 2012).

The fast evolution and aggressiveness of attacks highlights the vulnerabilities of private sector, which is required to put into action an improved protection and security of critical infrastructures, which are the first and greatest target of cyber war attacks and that are mostly privately owned (McAfee report, 2009).

4.1.4. CYBER WORLD AND ITS RULES

The increase of Internet importance in everyday life is reflected in the growth of Internet links which comprehend at this time more than 2 billion people worldwide (Internet World Stats, 2012) and more than 5 billion indexed pages (World Wide Web Size, 2014). However, as it increases the Internet, as the number of attacks and frictions grow and change the aspect of states and their relations. Digital conflicts, therefore, contributes to build up a new worldwide geopolitics, changing nations' characteristics and alliances and shaping international law because of new requirements and needs. Geopolitics reflects complex cultural relations and interrelations, in which identities and ways of thinking are grouped and expressed, but it is useful also in defining the source of danger and in providing security and protection, thanks to a better understanding and knowing of attacks (O' Tuathail, Dalby, 1998)

"*In some way, place is challenged. Ancient societies were built by distributing territory. Whether on the family scale, the group scale, the tribal scale or the national scale, memory was the earth; inheritance was the earth. The*

foundation of politics was the inscription of laws, not only on tables, but in the formation of region, nation or city. And I believe this is what is now challenged, contradicted by technology"

(Virilio, Lotringer, 1983)

Even if technology has been deeply studied and understood, a major challenge nowadays is to understanding the geopolitical context in which technology operates in order to give reasoning to cyber acts (Geers *et al.*, 2013). However, technology is gone beyond government or authorities control, but it is always more controlled and run by hackers, whose aim is to get around laws that censor the Internet and its inhabitants (Geers *et al.*, 2013), called *netizen* by Barlow (1996). In fact, the Internet is usually defined and perceived as a digital domain that embraces netizen and defend them and enhance them with large decision power (Barlow, 1996).

Cyber conflicts reflect "traditional" frictions and "traditional" tactics, at opposing blocks there is China and its strength given by number, and there are US, Russia and Israel whose attacks are surgical and technology-driven (Geers *et al.*, 2013). Cyber attacks, now, are creating several political risks and issues, as nations are increasingly dependent on critical infrastructures which are critically vulnerable to cyber attacks. Moreover, cyberspace is reflecting the collision between geopolitics and its force and cyber security and its employment. First of all, cyber space gives to states the capacity of expanding their power, even if military actions are not advised, because of high costs in human life and in weaponry. A clear and stunning example of the power of cyber attacks bended to politic motivations is Stuxnet attack, which hit Iran's industrial infrastructures that will be examined later in this chapter. Secondly, cyberspace becomes a battlefield for cyber attackers, aiming at supporting and continuing Julian Assange's objective of clarity and democracy, attacking governments and corporations.

It is possible to divide two main contrapositions in geopolitics arrays, refuge states and international alliances against these states (Antinori, 2011). Refuge states provide hospitality to cyber attackers, guilty of cyber attacks against

governments. These states are criticised at international level, for aiding criminals to prevent legal repercussions, but, at the same time, they gain global visibility for cultural and political reasons. In fact, on one hand, they stand up for cyber attackers, who may be seen by public opinion as democracy heroes, on the other hand, they show a high political maturity and great bargaining capacity, essential in order to resist at more powerful nations and international law enforcement (Antinori, 2011).

Consequently, countries constitute international allies against these refuge states through agreements, multilateral organizations and clear international law, in order to compact their political strengths and exercise greater pressure against refuge states. Thanks to these alliances, it is possible to prosecute cybercrooks at international level, which is the most effective tool in order to counteract organized and well structured criminality organizations (Antinori, 2011).

Analyzing the frictions between states and the methods and techniques used to perpetrate attacks will help the prevention of these attacks, and it will improve cyber security employed at national and private levels. Cyber space, therefore, become the battlefield of new conflicts and the new battlefield for old frictions, above all there is the US-China conflict.

China, due to its massive population and fast-growth economy , is "*the noisiest threat actor in cyberspace*" (Geers *et al*., 2013), it succeeds in cyber attacks thanks to brute force, a large volume of attacks, indifference in being prosecuted (Geers *et al*., 2013). It perpetrated several attacks against US infrastructures, here there are reported the most important, in terms of potential or actual damages, in order to give the idea of cyber geopolitics and its repercussions in everyday life. In 1999, China was accused by US Department of Energy to threat American nuclear security due to cyber espionage. Again, in 2009, China seemed to steal F-35 fighter jets plans, undermining technology advantage of US (Geers *et al*., 2013).

China targeted, during the years, several technology companies, such as Google, Intel and Adobe and it compromised a secured ID authentication technology threatening other more companies (Geers *et al*., 2013). Also business and financial institutions have been targets of China hackers, such as

Morgan Stanley, US Chamber of Commerce and numerous banks (Geers *et al*., 2013). China has perpetrated also attacks against media, maybe for propaganda reasons by manipulating or omitting stories and news (Egan, 2014). The chosen targets were The New York Times, Wall Street Journal and Washington Post, attacked using advanced and persistent cyber offensive techniques (Geers *et al*., 2013). In 2013, Chinese hackers hacked in order to sabotage them 23 gas pipeline companies, resulting in accidents and damages to US population (Geers *et al*., 2013).

Thanks to orchestrated attacks, China has access to sensitive information, including research and development data and information, to sensitive communications, such as from US Government and Chinese political dissidents, with the possibility of revealing their hidings.

However, China has global interests; consequently, it targets almost every nations in the world, in name of geopolitical conflicts, as Figure 4.5 shows the numbers of enterprises hit by Chinese cyber attacks

Figure 4.5: Cyber-attacks orchestrated by Chinese hackers

Source: Ritholtz B., Timeline of Cyber-Attacks from China, 2013, http://www.ritholtz.com/blog/2013/02/china-cyber-attacks/

Against Europe, China launched several attacks in order to strike the most significant institutions and retrieving sensitive information, such as attacking UK House of Commons. Also India is worried about the power of Chinese

cyber warriors, and the possibility of a Chinese attack against India Navy headquarters (Geers *et al*., 2013). While, South Korea is China target for years who attacks government computers; the most significant cyber attack against South Korea took place in 2011 when China assaulted an Internet portal who held personal information of 35 million Koreans (Geers *et al*., 2013). Japan too is targeted by China, who seeks information in government, military and high-tech networks (Geers *et al*., 2013). Instead, in Australia, China perpetrated a theft of the plans of Australian Security Intelligence Organization's new $631 million building.

China perpetrates, however, many other cyber plans, as Canadians researchers discovered a worldwide e-espionage in over 100 countries. Or, as it happened in 2011, when a Chinese telecommunications firm misrouted Internet traffic through China, exposing in this way 8000 US networks, 1000 Australian networks and 200 French networks (Geers *et al*., 2013).

Other countries using cyber attacks in order to redesign geopolitics and power are North and South Korea, representing two other major potencies, China who supports North Korea and its elementary cyber technologies, and USA, who supports South Korea and its technological advancements (Geers *et al*., 2013). The conflict between North and South Korea has arrived to cyberspace, and 2009 is the year of North Korea major attack on South Korea and US government websites, which resulted in few damages but it had a wide media exposure. South Korea also targets North Korea; in 2013 it provoked a two-day breakdown of websites hosted in the country. North Korea asked US and South Korea to take responsibility for the attack and the consequences derived (Geers *et al*., 2013).

Russia is another big cyber power, as it can have access to large funds and great national spirit, which improves cyber attacks in terms of targets quality and damages provoked (Geers *et al*., 2013). Russia used cyber attacks already in mid-1990s in Chechnya war; while Chechens advocated cyber propaganda, Russia was involved in shutting down their websites (Geers *et al*., 2013). In 1998, Serbia, an ally of Russia, attacked with DoS attacks NATO website and virus-infected email. Russia is suspected for the most punitive DDoS attacks

against Estonia, which suffered ten-day attack on Internet services, causing severe disruptions to banking system. The reasoning behind the attack was the punishment actuated by pro-Russia hackers against the entire country (Egan, 2014). Cyber warfare has an important role also in the invasion of Georgia in 2008, where Russia was able to integrate the kinetic warfare tactics of invasion with the most advanced cyber attacks in order to shutdown Georgia communications, in this way Russia impeded Georgia coordination and information and the involvement of international public opinion (McAfee report, 2009) (Egan, 2014).

Russia was the author in 2008 of the most significant breach of US military computers and networks (Geers *et al*., 2013), that used as attack vector an infected USB drive. Another breach took place in 2009, in which Russia breached university research paper about climate changes in order to undermine international negotiations; the operation is famous under the name of Climategate (Geers *et al*., 2013).

Also in the recent friction of Ukraine and Russia, it has been showed a combination of physical and cyber attacks in order to isolate Crimea from Kiev (Egan, 2014). In fact, it has been reported that armed men sabotaged fibre optic cables causing outages and service breakdowns. According to Director of George Washington University Frank Cilluffo (Egan, 2014), the actual actions are low-intensity cyber conflict, even if there is room for potential escalation of the conflict, due to Russia's sophistication and strong capabilities in cyber attacks.

As shown, North Korea, Russia and China are countries focused and interested in collecting cyber intelligence, in order to increase technological, commercial or political advantage with respect to other countries by stealing or breaching classified information, diplomatic positions and policy changes (Geers *et al*., 2013).

Cyber attacks of important magnitude require large funds; therefore the most significant attacks are perpetrated by US, Russia, Israel. However, Middle East, even if it does not have these large financial aids, has proved to be efficient in cyber attacks by relying on cyber tactics, which emphasize other characteristics rather than technical sophistication, such as novelty, creativity

and trickery (Geers *et al*., 2013). In 2012, Middle Eastern hackers used malicious documents, like Word, PowerPoint and PDF in order to infect targets.

A different issue is Syria, which is struggled in violent civil war, and the hacker group called Syrian Electronic Army (SEA), loyal to Syrian President Assad (Geers *et al*., 2013). SEA perpetrated DDoS attacks, phishing and spamming, it attacked by hackering Al-Jazeera, Anonymous, Associated Press (AP), BBC, Daily Telegraph, Financial Times, Guardian, Human Rights Watch, National Public Radio, The New York Times, Twitter and many other media. SEA was the author of fake announcement using Associated Press Twitter account claiming that White House was bombed and president Obama injured; this simple tweet affected stock markets (Geers *et al*., 2013). SEA, moreover, compromised in 2013 three widely used online communications websites such as Truecaller, Tango and Viber, these attacks give to Syria access to numerous communications and derived sensitive information to target political activists (Geers *et al*., 2013).

Israel is active in perpetrating cyber attacks while it is also one of the most targeted countries (Geers *et al*., 2013). Pro-Israeli hackers target politically and militarily significant websites in the Middle East, an example is the 2007 disruption of Syrian air defence networks perpetrated by Israel, which had repercussions also on domestic networks, in order to ease Israeli air attack against Syrian nuclear facility (Geers *et al*., 2013). However, the country proved to be vulnerable to external cyber attacks targeting Israeli economy. For instance, in 2009 hackers paralyzed numerous governmental websites through DDoS attack coming from 500000 computers (Geers *et al*., 2013), showing inefficiency of cyber security employed by Israel.

US is the force behind the most highly engineered cyber attacks that world has experienced, in fact, it is believed that US cyber intelligence is responsible for high-profile attacks, such as Stuxnet, Duqu, Flame and Gauss (Geers *et al*., 2013). Even if cyber attacks are characterized by anonymity and deniability, American orchestrated attacks are easily recognizable as require high level of financial investments, technical sophistication and legal supervision that cannot be attributed to other than US forces (Geers *et al*., 2013). However, USA has

still issues to be addressed in its defence tactics as it has been proved to be vulnerable to foreign cyber attacks. In fact, Iraqi insurgents would be able to intercept live video feeds from US drones, which give them the possibility to monitor and anticipate US military operations. Moreover, in 2011 International Monetary Fund, based in US, was victim of phishing attack which opened a breach to sensitive information (Geers *et al*., 2013).

Europe and NATO countries have given no indication of development of cyber warfare tactics, even if single European countries have at some extent cyber capabilities (Geers *et al*., 2013). However, European countries revealed to be targeted by other foreign countries, such as China and Russia. Significant examples are cyber attacks against UK government, which overcame network defence by pretending to come from and authorized source like the White House (Geers *et al*., 2013). Germany, too, was victim of cyber attacks by using phishing attacks which entered police servers which contained criminals and terrorism suspect's locations and information (Geers *et al*., 2013). Moreover, France was attacked by infecting Navy planes with a worm in 2009, while, in 2012, European Aeronautic defence and space company and German ThyssenKrupp were victims of massive attacks coming from Chinese cyberwarriors. In 2011, EU carbon trading market was breached in order to steal $7 million in credits, resulting in severe financial downturn (Geers *et al*., 2013). Therefore, nowadays, the European situation is changing, starting from UK and its decision to develop offensive cyber weapons as deterrence tool.

The cyberspace is, anyway, controlled and ruled by International Cyber Security law that regroups general legal terms and it applies them to cyber space and its relations. Thanks to this law, it is possible to divide responsibilities and rights between governments, in fact, delimitating areas of competence, States can exercise control over their jurisdictions and protect them (NATO Cooperative Cyber Defense Centre of excellence, 2013).
Rule 1 states that sovereignty indicates and delimits the area over which a State may exercise control over cyber infrastructures or CIIs (NATO Cooperative Cyber Defense Centre of excellence, 2013). Even if States cannot claim sovereignty over cyber space, this rule implies firstly that cyber infrastructures

are subject and bound to legal and regulatory control exercised by State, and secondly, that State's sovereignty protects these cyber infrastructures (NATO Cooperative Cyber Defense Centre of excellence, 2013). This principle gives to State the power of deciding whether restrict or protect access to the Internet, without corroding applicable international law and rights, such as human rights or international law about telecommunications (NATO Cooperative Cyber Defense Centre of excellence, 2013). Defined sovereignty, it is up to define jurisdiction, which expresses the authority of State over civil, criminal or administrative issues (NATO Cooperative Cyber Defense Centre of excellence, 2013). According to rule 2 of Tallinn Manual on the International Law Applicable to Cyber Warfare (NATO Cooperative Cyber Defense Centre of excellence, 2013), jurisdiction may be exercised by State over "*persons engaged in cyber activities on its territory; over cyber infrastructure located on its territory; and extraterritorially, in accordance with international law*" (NATO Cooperative Cyber Defense Centre of excellence, 2013). The principal prerequisite of applying jurisdiction is the actual physical or legal presence of persons or objects on State's territory, regulating personal cyber activities and activities of privately owned businesses. The challenge in defining jurisdiction is posed by cloud services and grids, which enlarge the national borders and blur jurisdiction's limits. However, as physical presence can be easily recognized thanks to geo-location techniques, it is useful to deepen the jurisdiction's definition and divide it in two terms, the first is subjective territorial jurisdiction and empowers State to prosecute according to its law and to exercise jurisdiction over initiators of attacks, resident inside national borders, then completed outside State's borders (NATO Cooperative Cyber Defense Centre of excellence, 2013); while, the second term is objective territorial jurisdiction which grants legal jurisdiction to the State "*where the particular incident has effects even though the act was initiated outside its territory*" (NATO Cooperative Cyber Defense Centre of excellence, 2013). This jurisdiction has revealed essential in law enforcement when Estonia and Georgia have been attacked, who were entitled to invoke jurisdiction as they suffer severe damages provoked by cyber attacks coming from outside their national borders. A different treatment of jurisdiction is needed for all those cyber infrastructures located on aircraft, ships or other moving platforms,

which are subject to the jurisdiction of flag State (NATO Cooperative Cyber Defense Centre of excellence, 2013).

Rule 5, instead, gives general behavior conducts that State should follow in order to maintain peaceful the cyberspace. In fact, this rule states that State should not allow that cyber infrastructures, located in their territory or under governmental control, are knowingly used for "*acts that adversely and unlawfully affect other States*" (NATO Cooperative Cyber Defense Centre of excellence, 2013). Since there are many difficulties in attributing and locating a possible attack, States may be forced to remedial actions such as self-denial, which consists in isolating and shutting down the network is supposed to be used (NATO Cooperative Cyber Defense Centre of excellence, 2013).

The document prepared by NATO Cooperative Cyber Defense Centre of excellence (2013) gives space also to self-defense law, as rule 13 states. This rule empowers of self-defense actions those State that are attacked through cyber operations, which can be considered and armed attack depending on scale and effects (NATO Cooperative Cyber Defense Centre of excellence, 2013). An attack is armed when presents trans-border elements, however it is not well defined who perpetrators should be. It is not clear if rule 13 of self-defense is applicable only when State targets another State, or it can be expanded to other frequent cases, such as a non-State subject that starts an attack to a State but his aim is not on behalf of another State (NATO Cooperative Cyber Defense Centre of excellence, 2013).

As cyber attacks represent a new and growing threat, therefore static international and domestic laws are not yet prepared to meet technical and political challenges (Hathaway *et al.*, 2012). Legal debates arise because of countermeasures needed when an attack is not considered armed and on strategies required in order to properly protect critical infrastructures. Therefore, it is evident that a clear and proper discussion about policies and law to be implemented is necessary and urgent. This clarity in legal and policy issues will help at defining the needed countermeasures and security processes that are "*legally and strategically appropriate for different types of cyber-attacks*" (Hathaway *et al.*, 2012).

4.2 SIGNIFICANT EXAMPLES OF THE DARK SIDE OF THE NET

This section aims at conducting a prospective analysis in order to conjugate a passive attitude towards incidents with anticipating forces in order to be ready for next severe cyber attacks (Prospective Analysis on Trends in Cybercrime from 2011 to 2020, 2011). In fact, the analysis of past events can help predicting behavioural and tactical paths of attackers, by increasing and improving knowledge about these techniques, it will be easier to recognize a cyber attack targeting your organization or at least it will be useful in order to improve cyber security implemented by businesses.
In this chapter, there are going to be analyzed the most significant and media-famous cyber attacks that struck the Internet and all its users.

The first worm that gained media attention because of its rapid spread is I LOVE YOU worm. It comes out in 2000 started from Philippines and spreads through email attachment toward Hong Kong, Europe and then USA; it attacks Windows personal computers. The attachment has a file extension of txt.vbs, while .vbs tends to be concealed by Windows by default. The worm limits its damages to local networks by overwriting image files and continues to spread as it copies itself and send to all addresses of Microsoft Outlook (McAfee report, 2010). I LOVE YOU holds the record as the most dangerous computer disasters, it infected more than fifty million computers, which represent 10% of Internet-connected machines, moreover, provoked at worldwide level an estimated damage of US $5.5-8.7 billion [5] and an estimate cost of US $15 billion (McAfee report, 2010), which comprehend time and efforts to remove the worm and to recover files. Bigger organizations, such as CIA, British Parliament and large organizations, decided in order to protect themselves from infection to shut down temporally their email systems.

After few months since I LOVE YOU worm, in September 2001 it comes out a new worm called Nimda, which uses numerous and different propagation techniques which make Nimda the most widespread threat over the Internet in less than 22 minutes. The date of release resulted to be suspicious and the

[5] I LOVE YOU, WHoWhatWhereWhenWhy.com

rumour has it that Nimda was an extension of terroristic act of Al Qaeda against USA (Hinde, 2001). This worm affects both workstation and servers running Windows (Hinde, 2001), as a combination of virus and worm, it is able to attack home computers, as well as large enterprises and as small business networks, and thanks to Trojan horse, Nimda can be spread by email as viruses, attacks directly computers because it is a worm and sneak in for looking for back doors, left open by previous infections, as a Trojan horse (Hinde, 2001). Since it resulted slower than other infections in spreading, it caused damages to organizations for about US$ 590 million[6], because security organizations were able to provide updated virus definition and protection.

Another mass infection is MyDoom worm which first struck in 2004, it is designed to infect computer and send spam emails. Due to large spread of this worm and enormous traffic provoked by spam sent, the global Internet traffic was slowed down and website accesses reduced by 50 percent (McAfee report, 2010), which cause billions of dollars in lost productivity and online sales (McAfee report, 2010). MyDoom was designed in order to perpetrate massive DDoS attack against SCO group website and through a second version of this worm against Microsoft website, even if it infected more than one million of computers, DDoS were not successful as the code, aimed at launching attacks, was functioning only in 25% of infected computers. However, MyDoom worm caused an estimated damage of US $38 billion (McAfee report, 2010), which represent the higher amount of damages provoked by computer threats. MyDoom comes back in 2009 during cyber attacks targeting South Korea and USA.

In 2007, there is Conficker worm which infected numerous computers (McAfee report, 2010) it is the largest known computer infection. It was designed to download and install malware from controlled sites. Conficker has the ability of propagating and forming botnet, which challenges security experts as it uses combinations of advanced malware, therefore it could affect government, business and personal computers in more than 200 countries. It

[6] Damage Toll for Nimda, less than was expected, 2001 http://www.xatrix.org/news/damage-toll-for-nimda-less-than-was-expected--773/

provoked damages for US $9.1 Billion, as it uses keystroke logger and other control software enabling cyber attackers to gain access to users' personal information and have free access to computers (McAfee report, 2010).

Since 2007, Zeus botnet is a serious threat to Internet users, its functionalities are stealing personal information by capturing data entered into websites (McAfee report, 2010) and creating the largest botnet in order to control infected machines (McAfee report, 2010), which are around 4 million of computers in USA. It is challenging as it is very difficult to detect as it hides itself in machine's codes which makes difficult for anti-virus software to detect it, moreover, Zeus worm counts 700 variants that are detected per day, challenging anti-virus detection capacities (McAfee report, 2010).

In 2007 a data breach occurred at TJX Companies, which provoked an estimated financial loss for US $ 1 billion and gave access to more than 45 million of personal records (Lockton, 2012). In fact, the company found out that it had used an unprotected wireless connection for 18 months; this gives the opportunity for a hacker, with simple tools and equipment, to have access to over 45 million credit and debit card numbers and personal data of thousands of persons (Lockton, 2012). The financial loss consisted of client notification, IT system restore, business interruption, fines, credit card repayments and legal costs, such a heavy burden and punishment that TJX learned to implement efficient cyber security and robust protection of customer data in order to prevent another data breach (Lockton, 2012).

In 2010 it was discovered Stuxnet worm, which targets critical infrastructures by exploiting Windows vulnerabilities (McAfee report, 2010). It was created in 2007 and was meant to attack Iran's nuclear facilities (Armerding, 2012), by ruining at least one-fifth of nuclear centrifuges[7], even if damages affected critical infrastructures also in India, USA and Indonesia (McAfee report,

[7] The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought, Business Insider,20 November 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

2010). It represents the first bridge cyber-created to real world, as it tangibly affects power grids, water supplies and other critical infrastructures (Armerding, 2012), leaving room for developments in cyber warfare techniques and tactics. Stuxnet works at three level, it uses a worm which executes main codes for the attack; then it intervenes a link file which automatically propagates copies of worm; and finally it is executed a rootkit component which aims at hiding malicious traces of the attack, therefore it prevents the detection of Stuxnet itself. The first infection contact takes place through an infected USB device, which propagates the worm across the network and ensures the existence of vital criteria; otherwise it becomes a dormant worm ready to be activated when all criteria are met. Because of this highly engineering structure, Stuxnet is supposed to cost for building around US $3 million, with unknown damages provoked.

Since 2009, a coordinated and targeted cyber attacks have been perpetrated against global oil, energy and petrochemical companies, starting the Night Dragon attack (McAfee Labs, 2011). The attacks includes numerous vectors of attacking, as social engineering, phishing, and exploitation of Microsoft vulnerabilities, Night Dragon works methodically and structures progressive intrusions in order to have access into targeted critical infrastructures. The attack started from China, whose hackers purchased hosted services in USA and the Netherlands in order to launch attacks against critical infrastructures, as well as hitting individual users and executives in Kazakhstan, Taiwan, Greece, and USA (McAfee Labs, 2011), in order to have access to confidential information. Instead, files about operational production systems and financial documents were copied or collected from SCADA systems, so collected by attackers (McAfee Labs, 2011). Night dragon focuses only on energy sectors, threatening social welfare and financial stability, however, a similar attack using and exploiting Night Dragon tools and techniques could be successful also if launched against other industries and critical infrastructures (McAfee Labs, 2011).

Another persistent cyber attack occurred in 2009 against Google, Adobe systems and other numerous companies in shipping, aeronautics, energy,

manufacturing, engineering and financial sectors. It has been conducted by a group of hackers in China (McAfee, 2010). The tactic used is water hole attack, which is perpetrated by infecting legitimate websites, which are normally frequented by employees, with malware which gives free access to infected machines and the network (McAfee, 2010). Thanks to the access, cybercrooks can search and download executives' emails and confidential documents regarding company plans, acquisitions plans and decisions. Moreover, it has been suggested that hackers aimed at finding out personal information about Chinese political dissidents by taking advantage of Gmail accounts. During this attack, hackers could obtain a part of Google's source code, which could weaken the competitive advantage of Google China *vis à vis* Baidu, Chinese competitor of Google (McAfee, 2010).

One of the latest threat coming from the Internet is called Project Blitzkrieg and it is about a mass fraud campaign against numerous US banks, which date of start should have been spring 2013 (Sherstobitoff, 2012), but the attack was called off since it was made public. The author posted the instruction of being part of the attack. It would have used Trojan horse in order to transfer from US banks million of dollars. This attack, that fortunately remained a threat, could be successful as it combines technicalities and innovation which are backed with successful tactics familiar to organized cyber crime (Sherstobitoff, 2012).

Attacks can be perpetrated because of moral and ethical positions, as Anonymous group is perpetrating since 2006 and its first great attack, the Habbo raid. Anonymous coordinates its actions between all its numerous activists through websites, forum and social media. By coordinated actions, in 2006 Anonymous blocked avatars from accessing pool in the virtual world of Habbo hotel (Paget, 2012); the motivation of this act was ambiguous, even if it is strongly believed that it was an act of protest against the lack of black characters and avatars in social network. In 2008, its efforts were directed against Scientology and its suppression of free-willing in members, by isolating them. The project is called Chanology project, and it is still going on. The principal weapons of Anonymous are responding actions to any attempt to regulate and censor the Internet (Paget, 2012). It combats by making

inaccessible significant and important websites, using attack software, which overload the targeted site saturating it though DoS attacks or DDoS (Paget, 2012). The freedom of the Internet is pivotal to Anonymous activists as they combat against censorships, copyrights limitation, in order to encourage information circulation and availability to public (Paget, 2012). This aim is the contact point between Anonymous and WikiLeaks, which is supported by the hackering capabilities of activists (Paget, 2012) in order to prevent the shutdown of WikiLeaks. The support to WikiLeaks is expressed in 2010 Operation Cablegate, in which Anonymous boosted the attention toward WikiLeaks as governmental and legal forces attempted to silence the site (Paget, 2012).

In order to fight back lobbies which gain from copyright materials and from the shutdown of Megaupload, Anonymous launched in 2012 the largest DDoS attack of the Internet history against several websites, such as US Department of Justice, Universal Music, Motion Picture Association of America, US Copyright Office, by involving more than 5000 participants (Paget, 2012). This attack showed the vulnerability of large corporations when public opinion is the principal perpetrator of attacks. In fact, Anonymous can exploit public feelings and the global reachability of the Internet in order to gather together numerous ethical hackers and forged them in order to perpetrate massive attacks. However, Anonymous can be seen also as a positive force, and not only a disruptive one, as it helped in 2007 at identifying pedophiles and at prosecuting them (Paget, 2012).

Since Anonymous has no leader, as it does not recognize authority within its ranks, public opinion often remained confused and skeptical about online threats, which are not transformed in actual operations or that are not well-orchestrated, indeed orders are followed by counter orders. In this category, there are few examples such as operation against US power grid or against DNS servers planned for 2012 (Paget, 2012), or the proposed operation Global Blackout in 2012 denied by official Anonymous twitter account (Paget, 2012).

However, this confusion and aggressive tactics make believe that Anonymous and activists are the most likely to attack organizations (Constantin, 2012), rather than cyber criminals, nation states, competitors and employees. Even if activists are responsible in 2011 to have stolen the largest quantity of data, they

represent, anyway, just 3% of total number of data breaches (Constantin, 2012). The reality is that the most used attack is malware, which is linked to cyber criminals, while DoS and DDoS are the attacks chosen by activists and Anonymous. The reason behind organizations' fear of Anonymous attacks is believed to be the negative publicity that Anonymous attacks produce and that have repercussions on organizations' image (Constantin, 2012).

This overview has the objective of highlighting the steps that composed a cyber attack and the security steps that are needed in order to prevent them or at least be ready and prepared at detecting them. In order to properly explain the next chapter about cyber security and its implementation, it is useful to understand practically cybercrooks techniques and tools, and to understand the financial damages and costs that would burden over organizations.

4.3 IMPLEMENTING CYBER SECURITY AS DETERRENCE FOR CYBER ATTACKS

By analyzing cyber threats it is possible to understand the importance of cyber space in daily operations and it is evident the vulnerabilities and the risks of not implementing an efficient security program. The heavy dependence that modern societies has built has strong effects on negative exposition to cyber threats (Thales, 2012), that as shown throughout chapter 4, may come from multiple and diverse sources and because of different motivations. According to a Ponemon Institute research (2013), cyber security threats are, for the negative financial impact and burden, as dangerous and scaring as natural disasters or business interruption. Therefore, cyber risks are threatening any entity that relies on ICT and CIIs, such as individual users, large, medium and small businesses, infrastructures, critical or not, and nation states, which are "*susceptible to cyber attacks that could paralyze their operations and leave them vulnerable to long-term damage*" (Thales, 2012). Cyber threats, however, grow directly dependent on the dimension of Internet (The Department of Commerce - Internet Policy Task Force, 2011) and therefore the steady growth of cyber or physical vulnerabilities that could be exploited by cybercrooks, in order to create damages, gain advantages and create buzz and confusion.

Cyber threats require awareness and improved security practices, which need to be shared by any users and to be aware. Therefore, it should be addressed the creation and implementation of robust culture of cyber security (Cornish *et al*., 2011) in order to create an homogenous basis of security which is shared by the majority of users. In fact, technology has to be supported with cultural and human factors, which must be trained, improved and empowered in order to offer a better protection of sensitive data and resources, which constitute a competitive advantage for organizations. Therefore, a cyber security strategy needs to focus on human aspects of organizations in order to make the approach robust and efficient for individual capacities and needs. In order to promote security culture in the organization by ensuring and providing best practices and tailored policies, that will help employees at identifying and avoiding risks, it is needed to establish a positive security culture which is able

to enrich and exploit employees' attitudes[8] by reinforcing them, eventually, by top management actions.

This positive culture can be enabled by basing it on trust rather than strict surveillance, which may exacerbate employees relationship with managers, but it is necessary to focus on acknowledging security breaches as opportunities to improve and learn, and to boost peer-to-peer encouragement in adopting just security behaviors. As security culture is centered on security seen as critical enabler to deliver an improved service to customers, managers and employees may be more inclined to enact cyber security throughout their actions and daily operations. This positive approach will have also positive effects and benefits throughout supply chain, inside and outside organization itself. In fact, by promoting security culture, employees, customers, suppliers and partners will be integrated and engaged in a proper security strategy that will benefit the overall society.

However, cyber security culture should be helped as it presents structural deficiencies (Cornish *et al*., 2011), due to asymmetrical economical incentives, which restrain a wider adoption of cyber security culture. In fact, incentives are unbalanced and do not motivate users and organizations to adopt the culture, which implies costs of training and implementing a new way of thinking and acting. By creating incentives it would be possible to motivate efficiently parties and players in the Internet economy (The Department of Commerce - Internet Policy Task Force, 2011), in order to invest sufficiently in cyber security, but without worsening competition, by creating entry or innovation barriers, or stemming economic growth or harshening of information flow inside and outside organizations (The Department of Commerce - Internet Policy Task Force, 2011).

Even if there is no uniform or shared approach to cyber security, few national or private organizations related to cyber security aim at providing standards and guidelines for organizations. For example, NIST (National Institute for Standards and Technology) provides a general framework adoptable by non-

[8] Chaffey N., People power: making your people an essential part of your cyber security strategy, http://www.paconsulting.com/our-thinking/why-a-human-side-is-essential-to-effective-cyber-security/

national security federal information systems (The Department of Commerce - Internet Policy Task Force, 2011), such as industries and agencies. It defines minimum security requirements for significant information systems and databases as well as CI and non critical ones. NIST framework helps at identifying the most suitable methods of security and protection according to organization's characteristics, and it provides businesses with metrics and methods for assessing the effectiveness of protection strategy (The Department of Commerce - Internet Policy Task Force, 2011). Moreover, it enables a trustworthy cooperation and information sharing between private companies and national agencies, and NIST, additionally, provides technical support for the implementation of security strategies, in order to ensure that strategies are consistent with antitrust laws, privacy laws, and that effectively limit vulnerabilities, prevent attacks, deter cybercrime by catching cybercrooks (The Department of Commerce - Internet Policy Task Force, 2011).

Another attempt of building a general framework in order to efficiently implement cyber security comes from Thales, a multinational company which addresses cyber assurance and security solutions to organizations. It considers cyber security as a principal tool for deterring cyber crime actions and cyber threats (Thales, 2012), as it is considered to be essential improving awareness of problems and their possible solutions. A proper cyber security is assumed to be the best incentive for allocating security investments, in order to be cost-efficiently and to not over-protect non-sensitive data or, worse, under-protect sensitive information (Thales, 2012). Therefore, Thales organizes a general framework with the principal assumption that security is composed of numerous layers that have to work together and consistently in order to ensure a complete protection of organization and its assets, so it creates the Four key pillars of cyber security strategy (Thales, 2012), which addresses four macro areas essential to organizations, which are information, people, communication and infrastructures (Thales, 2012). The interrelations which link these areas challenge further the protection and security of assets and processes of organizations.

By securing information, organization ensures its value, as information and data are for organizations the primary key assets and, if compromised or lost,

would represent a risk and a future costs or missed income (Thales, 2012). For securing people, the organization needs to train in depth employees and to transfer them with duty of care for them and their security (Thales, 2012). Another sensitive area is communication which has to be secured and protected both internally and externally through policies, procedures and trained staff. An example of protection strategy is encrypting in order to make difficult to steal records and information; it is, according to Thales (2012), a worthwhile investment comparing risks, possible costs and damage which are associated to a possible significant and important data loss (Thales, 2012). In order to protect and secure infrastructures, which are often outsourced, it is necessary to monitor critical networks and IT systems in order to keep an eye on traffic which enables the organization to detect and identify possible unusual behavior in order to respond rapidly and consistently (Thales, 2012). By adopting these general measures and precautions, it is possible to build an overall security strategy, which suits especially cyber security threats.

Therefore, it is possible to trace down few general guidelines which enables every organization and users to secure and protect their IT systems and information. In general terms, good practices are required, as they represent the level of cyber dependencies awareness, they reflect the knowledge and understanding of the supply chain and the long-term perspective the organization assumes in order to monitor risks and be prepared for respond to threats (Cornish *et al*., 2011). An example of good practice is empowering one person for security with the objective of increasing security awareness in employees, suppliers and customers; another good practice is to identify within organizational material and information those that needs and must be protected. Cyber security, however, is not made of security strategies and good practices but it needs to be integrated with the capability and agility of handling and coping with unexpected challenges and threats (Cornish *et al*., 2011).

According to Dr. Amoroso (2011), there are ten easily and intuitively recognizable and practicable principles. Deception is aimed at misleading a malicious attacker by "*creating a system component that looks real but it is in fact a trap*" (Amoroso, 2011), which is called honey pot. The principal aim of honey pot traps is to intensify and improve security even for those large critical

infrastructures, as they work on four pivotal points, cybercrooks' attention can be diverted, and their efforts and time can be wasted through fake targets, moreover, uncertainty is created around a real vulnerability, which is now less exploitable by malicious attackers, and honey pots can give a real time analysis of behavioral trend of attackers (Amoroso, 2011). Then, Dr. Amoroso enlists separation principle, by using a firewall in order to hide and protect information and IT systems, by increasing the complexity of an intrusion from outside. Diversity, moreover, can be used in order to protect and secure national and business infrastructures, diversity operates through the augmented resilience due to diverse infrastructures of IT systems. Thanks to a diversity strategy, it is possible for the overall ecosystem of organizations and critical infrastructures to be more resilient and more robust to attacks (Amoroso, 2011). But, at the same time, security strategies need to have common aspects, such as best practices, standards and tests, which create the security standards to be shared by organizations and infrastructures (Amoroso, 2011). Another principle is depth, which is referred to using multiple overlapping security layers of protection, with the objective of stopping, or at least, slowing down the cyber attack. This principle can be summed with the principle of discretion which adds depth and "obscurity" to security strategy. Collection is referred to the collection of any security-relevant data, which are useful in order to prevent, mitigate or analyze an attack (Amoroso, 2011). To this, it is linked correlation principle which, starting from collected data, compares data and monitors the timing of security software with, for example, detection and alarm system, which ensures an optimal and early detection of attacks (Amoroso, 2011). Situational awareness principle refers to collecting real-time data in order to understand the security risk posture and appetite of organizations, by taking into consideration and weighting technical, operational, business and global factors which influence organization's security risk (Amoroso, 2011). The tenth principle is incident response, which starts those processes by including security-related activities, initiated because of an "*imminent, suspected, under way or completed"* (Amoroso, 2011) cyber-attack. By adopting these principles, it is possible to sensibly reduce cyber attacks, or at least reduce their damages and costs which burden organizations and critical infrastructures.

Cyber-attacks need to be more elaborated in order to be able to manipulate and damage critical infrastructures, and therefore such attacks require time, efforts and expertise of considerable extent (Geers, 2009). A growing concern is the protection and security of control systems, like SCADA, against malicious attacks. The protection of these systems could be incentivized by cooperation between asset owners and vendors, in order to boost the implementation of best security practices (Càrdenas *et al.*, 2009). The ongoing strategy more adopted is to focus on reliability, ensured against random faults that SCADA may meet. However, a more comprehensive security strategy includes the importance of detection and response to attacks, by monitoring physical system and checking anomalies detectable, which can indicate under way attacks (Càrdenas *et al.*, 2009). Detection process is fostered by information awareness of control system operators, in order to promptly recognize any cyber threat or attack, through training, implementation of protocols and guidelines that will help operators in detection and response processes (Càrdenas *et al.*, 2009). General principles, that can be implemented in order to make SCADA and other control systems robust and resilient in case of attacks, are increasing redundancy in order to prevent single-point failure, redundancies can be physical and analytical which need to be combined with other security principles, such as diversity and separation principle; or boosting diversity, in this way replicas, due to redundancy, are not compromised by a single vector of attacks, which increases resilience (Càrdenas *et al.*, 2009); in order to limit privileges of a corrupted entity it is required to adopt principle of least-privilege and separation of privilege (Càrdenas *et al.*, 2009). Another security strategy may be deterrence, but it depends on legislation, law enforcement and international collaboration, which collaborate in order to bypass the attribution problem and ease criminals tracking, however, this strategy still needs to be developed (Càrdenas *et al.*, 2009).

Consequently, in order to ensure the maximum protection and cyber security to critical infrastructures, NIST builds a framework which enables any organization to "*apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure"* (NIST, 2014). Even if this framework does not provide a one-size-fits-all solution, it provides

organizations with standards, guidelines and best practices that can adapt to their unique risks, threats and vulnerabilities, creating a tailored cyber security strategy for critical information (NIST, 2014). The common steps and taxonomy are constructed throughout five points; the first point concerns describing current cyber security approach; then it needs to be described the targeted objectives for cyber security. Consequently, it is required to identify and prioritize opportunities for improvement, as the process is continuous and repeatable (NIST, 2014). During the process, critical infrastructures owners and managers are required to assess the progress toward the target objective of cyber security (NIST, 2014). The final step is as important as the others, since it requires communicating to the stakeholders the cyber security strategy, results and risks that are not yet secured by the cyber security (NIST, 2014).

The framework proposes itself as a complement of organization's risk management strategy, which has been showed in chapter 3. If the organization has already implemented a cyber security strategy, the organization can use the NIST framework as benchmark, in order to align results and objectives with industry practices. Instead, organization without an existing cyber security strategy can use and implement framework as a reference in order to construct its own strategy (NIST, 2014). Moreover, the implementation of risk management practices offer and enable organizations with the capability of quantifying and then communicating results and needed adjustments to cyber security programs(NIST, 2014).

As cyber security actions, it is useful to analyze briefly other defenses that organizations may undertake in order to secure IT systems and data.

As passive cyber defense, it is worthwhile mention firewalls, which are required for implementing Dr. Amoroso (2011) cyber security strategy, intrusion detection or prevention systems, and auditing activity registers in order to understand risks and vulnerabilities.

On the other hand, there are active defenses which imply the employment of limited range of offensive actions in order to stop an enemy at gaining advantageous area or position, and they can categorized as cyber exploitation, counter attack, preemptive attack, preventive attack and cyber deterrence. Cyber exploitation exploits computer systems which are involved in cyber

attack in order to retrieve data and information which can help and facilitate the analysis of the attack and the determination of attribution. The second category is counter attack (Finklea, Theohary, 2013) which is define by US Department of Defense as an attack against an enemy attacking force, adapting this definition to cyber attacks, a possible process of counterattacking is hacking the attacker in order to block or at least neutralizing the attacker's force. Preemptive strikes can be used when the attack is believed to be under way or imminent, therefore the victim attacks first the attacker in order to not suffer damages or limit them. According to Sofaer (2010), a preventive strike is described as "*use of force against an anticipated attack based on a judgment that the attacker will use existing or potential means to attack in the future, or to engender other types of harm, including, for example, harm to hostages, attacks by non-state actors, or the mistreatment by a State of its own nationals"* (Sofaer, 2010). This definition implies that the attack as defense is launched before any offensive attack, which makes possible to launch a defensive attack against a hostile actor in order to prevent this from acquiring further cyber offensive capacities, which constitutes a real threat to the defending attacker (Sofaer, 2010).

Around these active cyber defense actions there is an international debate about whether these actions are justified, as they can be perceived as controversial under certain international laws. Moreover, the controversy is extended to the non-regulated recourse to these defense strategies, which appears as hostile as offensive, that always more organizations use in order to prevent physical and financial losses (Katz, 2013 a). In fact, "*there are organizations that are beginning to develop the capability of identifying the bad guy using intelligence. It's sort of like a mini-CIA*" (Katz, 2013 a), as organizations can now launch DoS attacks or malware against servers hosting potential cybercriminals. Organizations exploit the cooperation with telecommunications companies which help them to detect and attribute the attack even if perpetrated from outside national borders (Katz, 2013 a). However, it is to notice that there are still organizations that trust the cooperation with governments and national agencies in order to model an efficient attack, by collecting and sharing data and information (Katz, 2013 a).

Cyber deterrence, conversely, is another active cyber defense action, which reprises a military action which aims at maintaining the status quo, by designing a threat which scares the deterred party of changing the status quo (Schelling, 1966). The forms of deterrence present two main issues that challenge national security, attribution of the threat origin and asymmetry of cyber capabilities and strategies (Geers, 2010), which influence deterrence defense strategy.

Deterrence by denial is a strategy which contributes to prevent enemy's acquisition of threatening technology (Geers, 2010), by preventing to gain advantages from first-mover benefits (Kramer, 2014). The requirement of employing cyber deterrence involves deep evaluation of human psychology and behavior, foreign political and military affairs (Geers, 2010), since the threatened party needs to be sure that the threat of retaliation or of pre-emptive strike is real and incumbent.

Cyber deterrence can assume the form of deterrence as punishment, which is meant to be a last resort strategy, since it is implemented when deterrence by denial is not enforceable or failed (Geers, 2010), so threatening party has been successful in acquiring the technology that represents a real threat. Deterrence by punishment aims at preventing a possible aggression by threatening an aggressive and preventive attack (Geers, 2010).

Another form of defense is cyber sanctions, which work as a deterrence especially for cyber espionage by raising fines or the riskiness of the malicious act (Kramer, 2014), consequently, they act as a further cyber security strategy in order to protect organizations and users. They present three main benefits to nations which should incentivize the adoption of cyber sanctions supported by cyber international law. Firstly, sanctions would raise the expected costs of malicious attackers (Kramer, 2014). Then, they would be a strong signal to those countries which encourage or support cybercriminals (Kramer, 2014), such as refuge states discussed at point 4.1.4. The last but not least benefit is that sanctions will encourage and authorize private initiatives which support and integrate governmental actions in order to activate more efficient and effective strategies aimed at cyber security (Kramer, 2014).

It has been showed the most actuated forms and strategies of cyber defense undertaken by States, organizations and critical infrastructure owners in order to prevent or mitigate damages of cyber attacks. The frameworks help managers and strategists to construct and apply a suitable and tailored cyber security which is consistent with factors, such as economical, political and cultural. Moreover, it has been showed the importance of supporting cyber security strategy with security culture which has to be shared and absorbed by employees at top, middle and low level, in order to ensure a strong and consistent security strategy applied at cyber space. Implementing basic principles at IT system infrastructure, as dictated by Dr. Amoroso (2011), is able to ensure an efficient cyber security for the most technological structures, such as critical infrastructures which need a special and more focused security and defense in order to avoid severe damages for society. Furthermore, cyber security has been strictly linked to national security, as nations and governmental functions are run on computers and IT infrastructures.

At this point, the organization which runs critical infrastructure has employed an efficient CIP and CIIP, it has assured the information supply chain and secured its cyber infrastructures against cyber crime, ensuring stakeholders and insurance operators that the organization has low likelihood of suffering severe damages provoked by cyber criminals. By implementing these protection and security strategies, an organization is reassuring and stating its risk appetite in order to successful underwrite a cyber insurance which helps to mitigate unexpected or residual risks and damages, which are unprotected through all the security actions undertaken.

Chapter 5

THE ECONOMICS OF CYBER INSURANCE

Chapter five introduces the importance of cyber insurance, which transfers cyber risks to an insurance company that can effectively and profitably mitigate risks in return of premiums. In fact, as the importance of the Internet grows, firms are more vulnerable to threats and risks coming from cyber criminals, who attempt to gain unauthorized credentials and access to sensitive information, causing significant financial and business losses to firms. However, cyber insurance proves that, if effectively implemented alongside with cyber security strategies and risk management procedures, it is a valid ally for mitigating those risks that remain uncovered by normal security strategies. Moreover, cyber insurance may affect positively other industries and users, thanks to improved cyber security spread over the Internet and IT infrastructures.

In **An Overview of Cyber Insurance**, there are presented the principal characteristics of cyber insurance, by analyzing general coverage offered by insurers and side effects typical of insurance, such as moral hazard and adverse selection. Cyber insurance is gaining importance and focus from firms and insurance companies, since it may increase the overall network safety and protection since the insured tangibly increases and improves self-defense strategies. Particular focus is posed on critical infrastructures, that, due to their complexities and interdependencies, can be attacked and damaged from numerous sources, as they can be downed due to physical events, and, moreover, through the cyber space. In fact, cybercriminals can damage CI functionalities by striking SCADA systems, or by causing cyber-related events. Insurance is required especially for cloud computing service providers, against cyber terroristic attacks, and for protecting control system, such as SCADA. The cyber insurance applied to critical infrastructures may act as a facilitator tool in order to collect information and risk assessment, enabling insurers with greater information power as they can improve insurance conditions, terms and premiums.

In **Improving Cyber Insurance**, they are listed and briefly analyzed some of the most used models in cyber insurance. These models are exposed in order to examine the different characteristics that are offered by insurers who tend to maximize the total outcome as a function of clients, thanks to the mitigation offered by the insurance company; of insurers, as they collect an higher premiums and do risk less and of society, as the improved protection may ensure the totality of users of better status of the Internet and provided services in case of CI.

In **Evolution and Challenges of Cyber Insurance**, it is highlighted the importance and future trends that may face cyber insurance market. In fact, cyber insurance market, thanks to its novelty, leaves large room for adapting its conditions and terms to changing needs of firms and users in order to propose new models of insurance according to firms' budget and risks. In conclusion, cyber insurance has to address challenges in order to improve and boost its adoption towards firms and industries. In fact, an increased adoption of cyber insurance is proved to improve the Internet conditions for the majority of users, even those that do not purchase cyber insurance. However, the booming of cyber insurance market requires legislative developments and improvements in order to address properly investments in cyber security.

Chapter 5

THE ECONOMICS OF CYBER INSURANCE

5.1 AN OVERVIEW OF CYBER INSURANCE

As the Internet and technology improve and their importance grows, organizations and users find out the danger and threat coming from the dark side of the Net and technology, since they can be easily exploited by cybercrooks and cyber terrorists provoking damages and costs to businesses and society. In fact, technological advancements, a broader Internet access and evolving IT systems offer significant and advantageous benefits and opportunities to businesses (Capgemini, 2012), which are more empowered in order to satisfy and meet adequately customers needs, but, however, the increased use of technology poses a big challenge to the market as it increases the risk of cybercrime attacks, with significant financial and non-financial consequences and implications for organizations (Capgemini, 2012).

For this, a growing number of businesses adopt and employ cyber-security measures and strategies, combining technology and security countermeasures in order to prevent cybercrime incidences and larger consequences. However, cyber security procedures, that are shown throughout this dissertation, such as information assurance and cyber security strategies, need to be sided with other deterrents as these cyber security strategies cannot prevent all potential attacks, which are always more aggressive and resourceful.

Since there is a growing dependency on technology and an increased threat of unauthorized access to data and information, there is also a response of insurance market to these challenges, backed by an increased awareness and knowledge of corporations about cyber risks and exposure (Airmic technical, 2012), consequently, the potentiality of insurance results significant for organizations as a control mechanism. Alongside with preventive measures, the mitigation of financial risks faced by businesses can be acts in two ways (Capgemini, 2012), the first consists in assuming risks internally by setting aside funds which are available to compensate the potential future loss (Capgemini, 2012), and it is self-insurance, but it also risky as it needs an

accurate estimation of loss in order to construct a proper fund, for this difficulty it is emerging the area of cyber insurance, which transfers risk to external insurance company by purchasing cybercrime insurance (Capgemini, 2012).

Cyber insurance is enacted through the transfer of network user risks to an insurance company, which can mitigate the risks, in return of a fee or premium (Pal, Hui, 2012). It goes by many times, since cyber insurance is a generic term which includes numerous coverages, it is going to be listed some examples of policy coverages. Network security coverage covers against claims of third parties who were economically harmed by a data breach or identity theft suffered by the organization (Bernard, 2008). Another possible insurance is digital media liability which covers for exposures related to misuse of trademarks, domain names and protects against plagiarism, copyright infringement and defamation (Bernard, 2008). Digital business income coverage, instead, helps in case of income loss due to network intrusion and inaccessibility or damages to IT system (Bernard, 2008). Crisis management coverage gives economic relief and help for handling public relations afterwards a security breach (Bernard, 2008). Moreover, there are proposed also insurances against cybercrime acts, such as internal criminal acts coverage, which indicates cyber criminal activities perpetrated by employees; hackers coverage which insures against malicious attacks directed to company's networks and IT systems or that use organization as a platform for launching third-party attacks (Bernard, 2008); and it has been studied and proposed a coverage against the cost associated to virus, worms and Trojans attacks, explained in chapter 4.1.1., which cause interruption of business routines and require the reconstruction of lost or damaged data or infrastructures (Bernard, 2008).

Cyber insurance is gaining always more importance and focus from businesses and insurance companies, since a broader subscription of cyber insurance can have different and positive benefits for society. In fact, cyber insurance can theoretically increase the overall network safety and protection as the insured party increases and improves self-defence strategies in order to meet fewer risks and, therefore, to lower insurance premium (Pal, Hui, 2012). Cyber

insurance will lead the market to a solution by aligning economic incentives of cyber insurers with users and security software vendors (Pal, Hui, 2012), as "*the cyber insurers will earn profit from appropriately pricing premiums, network users will seek to hedge potential losses, and the software vendors could go ahead with their first-mover and lock-in strategies*" (Pal, Hui, 2012). Moreover, thanks to cyber insurance, it is needed an adequate protection and security, instead of costly and impossible absolute protection, which transfers risks to third party (Pal, Hui, 2012).

Therefore, cyber insurance in order to mitigate and offer better coverages requires an improved estimation of risks and their costs and a better design in order to transfer suitable amount of self-defence, proper liability on clients which in turn makes the overall cyberspace more robust and resilient benefitting users (Pal, Hui, 2012).

However, insurances may incur in classical problems which toughen the terms of insurance, these problems are adverse selection and moral hazard, and can result problematic also in cyber insurance market, as they are part of principal-agent problem and asymmetric information problem. Moral hazard occurs when the insured-agent can influence and affect the expected value of the loss thanks to his/her ability to modify the probability of undesirable event, or the magnitude of the loss (Rowlands, Devlin, 2006), so, due to asymmetric information, agent's actions are unobservable to the principle-insurer, leading to excessive burden of costs at the expense of insurer. In addition, adverse selection is due to asymmetric flow of information between principal and agent, in which the agent has more information about the risk and does not share with the insurance company the likelihood of negative event (Rowlands, Devlin, 2006).

At this point, it is useful analyze and understand cyber risks and the impact on cyber insurance underwriting. In fact, cyber risks vary extensively according to threat, vulnerability and consequences, therefore, not all risks can be insurable by insurance market. There are insurable risks, uninsurable and partially insurable, this variability requires a careful study of industry and cyber threats faced by organizations, in order to avoid the ruin for the insurer (Bolot,

Lelarge, 2008), which is met when premium are lower and insufficient to cover the possible claims.

The insurable cyber risks are liability due to data breach or loss of data or information, notification and other costs related to data breach, network damages and cyber extortion, some regulatory issues which need to be selected and analyzed according to regulator and type of data involved in regulation (US Homeland Security, 2012). When risks are correlated, interdependent and strictly linked as it happens for the Internet risks, insurers tend to refuse to covers such risks, as these risks are less attractive and more risky for insurance companies, moreover, these risks are less estimable since single decisions about security investments and self-protection affect the remaining risk faced by other users (Lelarge, Bolot, 2009).

However, the challenge for insurers is to mitigate and estimate the uncertainty about cyber risks, moreover the insurance market tends to be driven towards clients' requests which are limited to coverages that respond to the latest cyber incidents rather than focusing on more forward-looking and comprehensive policies (US Homeland Security, 2012). This limitation in providing more comprehensive and different coverages limits and deprives insurers of the "full benefit that risk transfer could play in their cyber security risk management strategies" (US Homeland Security, 2012), weakening the insurance market and limiting the protection offered to clients.

Traditional insurance policies may cover cyber risks, including commercial general liability coverage (Anderson, 2013). This coverage provides protection against liability due to claims alleging physical injury or property damage and also claiming personal injuries and advertising liability (Anderson, 2013). Even if this coverage does not intend to cover cyber risks, insured parties may have the possibility to success in pursuing this traditional coverage also for cyber risks; in particular cases, coverage has been ensured against cyber risks according, however, to each particular case, on the basis of terms and conditions of contracts and applicable law. However, it is argued that data and software cannot suffer physical injuries and therefore property damage, since they are not tangible property (Anderson, 2013). However, numerous courts have disagreed to this conception of data as intangible property, and,

consequently, data and software can suffer physical injuries, and be covered by commercial general liability coverage (Anderson, 2013). Moreover, according to personal and advertising injury liability coverage, insurers are obliged to pay those sums legally requested to insured party (Anderson, 2013).

Figure 5.1 : Cyber insurance policies comparison

Risks	Coverage	Traditional Policies	Cyber & Privacy Policy
Legal liability to others for privacy breaches	Privacy Liability: Harm suffered by others due to the disclosure of confidential information		
Legal liability to others for computer security breaches	Network Security Liability: Harm suffered by others from a failure of your network security		
Loss or damage to data/information	Property Loss: The value of data stolen, destroyed, or corrupted by a computer attack		
Loss of revenue due to a computer attack	Loss of Revenue: Business income that is interrupted by a computer attack		
Extra expense to recover/respond to a computer attack	Cyber Extortion: The cost of investigation and the extortion demand		
Loss or damage to reputation			
Identity theft	Expenses resulting from identity theft		
Privacy notification requirements	Cost to comply with privacy breach notification statues		
Regulatory actions	Legal defense for regulatory actions		

Not typically covered May be covered Typically covered

Source : Marsh, Cyber Risk: Trends And Solutions, 2013

A shown in figure 5.1, the majority of policies covers cyber-related incidents and losses caused to third parties, few companies offer a coverage for first-party losses, such as income loss due to downed or damaged networks, expenses for restoring IT systems and reputational damages, which still burden the organization (US Homeland Security, 2012). However, it results that the market is ready and open to both first-party and third-party risks (US Homeland Security, 2012).

First-party insurance provides protection for the property owned by the insured, it would cover costs of restoring lost data or lost business and reputational harms helping through payments when the property suffers damages or losses (US Homeland Security, 2012) (Airmic technical, 2012). First-party insurance are commonly theft insurance, fire insurance and protection against losses caused by earthquakes or flood, consequently, is complementary and relevant to cyber risks, since it provides protection and relief against financial consequences to the most common cyber threats that organizations may incur, as exposed in table 5.1.

Table 5.1 : First-party cyber risks exposures

1.	Loss or damage to digital assets – loss or damage to data or software programs, resulting in cost being incurred in restoring, updating, recreating or replacing these assets to the same condition they were in prior to the loss or damage
2.	Business interruption from network downtime – interruption, degradation in service or failure of the network, resulting in loss of income, increased cost of operation and/or cost being incurred in mitigating and investigating the loss
3.	Cyber extortion – attempt to extort money by threatening to damage or restrict the network, release data obtained from the network and/or communicate with the customer base under false pretences to obtain personal information
4.	Reputational damage – arising from a data protection breach being reported (whether factually correct or not), that results in loss of intellectual property, income, loss of customers and/or increased cost of operation
5.	Theft of money and digital assets – direct monetary losses and associated disruption from theft of computer equipment, as well as electronic theft of funds / money from the organisation by hacking or other type of cyber crime

Source Airmic technical, Airmic Review of Recent Developments in the Cyber Insurance Market & commentary on the increased availability of cyber insurance products, 2012

Conversely, third-party insurance is relevant when organizations face significant exposure to cyber threat because their IT systems have damaged a third party involved or have lost their data and information (US Homeland Security, 2012). Sometimes policy coverages include also assistance or management of the incident and a further financial compensation for the cost of the incident, this inclusion and wider offer of insurance plan may be an important key and valuable aspect for organizations, especially if they expect a possible incident with a high damage potentiality to reputation or that may result in regulatory enforcement (Airmic technical, 2012). Cyber risks are related to the company's nature and core business, since they can range from risk of data loss to data corruption due to performance of external professional services, while other risks are presented in table 5.2.

Table 5.2: Third-party cyber liability exposures

1.	Security and privacy breaches – investigation, defence cost and civil damages associated with security breach, transmission of malicious code, or breach of third-party or employee privacy rights or confidentiality, including failure by outsourced service provider
2.	Investigation of privacy breach – investigation, defence cost, awards and fines (may not be insurable in certain territories) resulting from an investigation or enforcement action by a regulator as a result of security and privacy liability
3.	Customer notification expenses – legal, postage and advertising expenses where there is a legal or regulatory requirement to notify individuals of a security or privacy breach, including associated reputational expenses
4.	Multi-media liability – investigation, defence cost and civil damages arising from defamation, breach of privacy, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party
5.	Loss of third party data – liability for damage to or corruption / loss of third-party data or information, including payment of compensation to customers for denial of access, failure of software, data errors and system security failure

Source Airmic technical, Airmic Review of Recent Developments in the Cyber Insurance Market & commentary on the increased availability of cyber insurance products, 2012

The risk exposure of businesses arises due to the interdependency of more networks and machines and to the frequent use of outsourced services, such as cloud computing, affecting their own activities and third-party service providers (Airmic technical, 2012). Therefore, it is required to undertake a complete risk assessment in order to identify and assess third-party risks, moreover it is necessary to improve and facilitate the discussion and information flow between IT specialists and risk managers in order to properly identify third-party liability exposures, listed in table 5.2. From the legal point of view, it may be important and required to ensure that strict and clear contract terms and conditions are present in the contract and in place, in order to reassure risk bearer, *i.e.* the insurer (Airmic technical, 2012).

These considerations represent broadly speaking the cyber insurance and its market. This first explanation is useful in order to introduce the importance of cyber insurance in everyday business and life, as cyber risks are extensively threatening any Internet users and society, due to the growing dependency on the Internet communications. The estimation of cyber threats cost is around £20 billion per annum for the UK economy (Airmic technical, 2012). A further estimation of foreseeable cyber threat costs is around £250,000 due to business interruption, and in general a cyber event may costs around £500,000

(Airmic technical, 2012). Consequently, for US market a typical premium may cost $100,000 for a maximum indemnity of $10 million, by providing coverage of first-party and third-party risks and liabilities. Of course, the market affects the premium and the costs of cyber insurance, as, for example, an organization, which does not have an US exposure, may pay £30,000 for an indemnity of £1 million, or a premium of £150,000 for a £10 million limit (Airmic technical, 2012).

Thanks to a growing awareness and focus on cyber aspects of organizations and businesses, the insurance market is flourishing as just in the US market the totality of premium reaches $500 million, which increases the product development investments and the capacity for cyber risk exposure (Airmic technical, 2012).

Therefore, insurance is beneficial for more markets and players at once, since it protects businesses, assures a robust Internet, provides further investments in protection and security and it may reactivate the overall economy.

5.1.1. CRITICAL INFRASTRUCTURES NEEDING CYBER INSURANCE

A special focus is needed in order to explain the relation between critical infrastructures and cyber insurance. As any other business, critical infrastructure needs a global protection in order to reassure clients and stakeholders that the service provided can be resilient to any adverse incident and be brought and continued. In fact, critical infrastructures, due to their complexities, can be attacked and damaged from numerous sources, they can be downed due to physical events, such as floods, fire and structural failures, but they can be also attacked trough the cyberspace, damaging their functionalities by striking SCADA systems, cyber attacks that can cause cyber-caused events. As showed throughout chapter 1 and 2, critical infrastructures are sensitive targets which are interdependent and dependent on each other. Moreover, Internet-enabled technologies are crucial for everyday life and business, since it is critical for operating SCADA and other control systems. Critical infrastructures, therefore, represent a target for cybercrooks, which threaten not only these infrastructures but also the entire society and its well-

being and functionality (US Homeland Security, 2012). In fact, data and information are the input and output of critical infrastructures which are valuable for cyber attackers, due to their economic value and for their impact value on society and business.

For the value of data, cloud computing is one big challenge for insurers and clients, since there is a lack of clarity about who is responsible for losses in the cloud (US Homeland Security, 2012). Moreover, cloud computing services represent a further risk because the strict number of dominant platforms of cloud services sustain a large amount of data and information, increasing the aggregation risk, that can harm and cause potentially large and significant losses (US Homeland Security, 2012), since thousands of users could be affected simultaneously by cloud service platform failure (US Homeland Security, 2012). Therefore, cloud service providers are recognized as responsible for cyber security vulnerabilities, as they result causing one-third of cyber incidents.

The actual situation about liability accepted by cloud providers for cloud-related losses is pouring extra risks on companies and clients of cloud computing services. Indeed, providers accept liability limited to the service that is provided, even if some cloud providers agree to recognize losses regardless of service limitations by purchasing errors and omission insurance in order to transfer liability risks to the insurance company (US Homeland Security, 2012). However, cloud computing clients are asking more clarity and transparency about the risks that are covered and which is not in basis of the cyber security capabilities of cloud providers (US Homeland Security, 2012*),* consequently, this deeper examination of cyber security capacities would assess the capabilities and strategies in order to protect and secure clients' data and information and, therefore, it would mean a lower premium for those cloud computing providers that enact a stricter and more effective cyber security (US Homeland Security, 2012).

A great preoccupation for critical infrastructures owners are terroristic threats, since critical infrastructures are sensitive targets with a high impact effect on society's well-being and fear. Even if it is assessed that US Department of

Homeland Security has sponsored numerous safety programs addressing anti-terrorism protection oriented to kinetic threats, fewer efforts are endeavoured towards cyber threats due to terrorism, which are always more a tangible and worrying threat to CI. Consequently, CI owners and operators have implemented good practices for addressing kinetic terroristic threats, by hiring experts who could provide them with "*robust command and control capabilities*" (US Homeland Security, 2012), such as sensors and guards, that may decrease the likelihood of such attacks. But, CI operators are still confused about the proper cyber security actions that they can undertake in order to secure and protect their infrastructures, in fact, they are trying to adopt and adapt metrics, requirements and standards to their operational needs and quality assurance (US Homeland Security, 2012).

Moreover, about critical infrastructures, it is difficult to assess and address the responsibility for risks that CI face; this situation is often resolved thanks to self-insurance practices undertaken by CI owners and operators, however this solution is not a market-driven solution but it is just a procrastination of the primary problem of risk attribution and consequently liability and investment burden. Insurance policies tend to exclude terrorism and war terms, even if insurers may not deny a cyber-related claim if there is or was a clear and expressed terroristic act, or if "*more specific exclusion addressing cyber terrorism or war is included in the policy*" (US Homeland Security, 2012). What is sure is that, since it is impossible to make a claim against a nation state, that is proved to be behind the attacks, which pays the loss due to the negative outcome of attacks addressed to CI are financial institution, insurers and consumers (US Homeland Security, 2012).

Under these market's imparities, there are some stakeholders that would ask to the government to accept liability for cyber risks faced by CI owners and operators (US Homeland Security, 2012). In fact, if critical infrastructures cannot handle the excessive loss due to cyber attacks, it would be up to the government to address it and help CI (US Homeland Security, 2012), by building a fund which is aimed for addressing cyber-related CI losses, which would equate cyber risks to flood and other natural losses beyond organizations' strengths. However, this proposal of government aids provokes different reactions in critical infrastructures representatives in a roundtable

organized by US Department of Homeland Security (2012). In fact, there are historical records of other companies that stepped in to help other critical infrastructures severed by losses, leaving out the government aids and its liability for risks.

The position of the government, expressed by a Federal government participant to the roundtable (2012), states that the only duty of the government is to provide additional and accurate information to CI owners and operators about new or increased cyber threats (US Homeland Security, 2012), in order to allow insurance companies to require improved cyber security to CI.

All these assertion bring to a new concept about cyber security, which is not anymore focused on prevention but on risk management, which has been fully analyzed in chapter 3.3. By implementing a cyber security risk management, the principal aim for organizations is to cause difficulties to malicious activities in order to deter the attacker. In order to have a short and efficient response time, corporate risk managers are increasingly using predictive analytics in order to increase and improve their cyber risk preparedness (US Homeland Security, 2012). Thanks to experience, stakeholders have developed processes that help identifying the likelihood of a cyber attacks and quantifying risks and costs. From insurers' point of view, companies are grouped according to geographical and sector basis, as different industries are exposed to attacks of different nature or magnitude (US Homeland Security, 2012). While, according to critical infrastructures operators, it is recommended to assess the frequency and the severity of damages caused by cyber attacks, in order to forecast risks, costs and investment budget. Moreover, it is helpful to build strong and bidirectional relationships with stakeholders "*who have actionable and trustworthy threat intelligence about the risk*" (US Homeland Security, 2012).

SCADA systems represent the most common control system implemented in running critical infrastructures, and therefore, due to their importance to the overall status of CI. Insurers argue that a general liability policy could cover physical losses that resulted due to a cyber incident, therefore it is not clear if the relation between physical and cyber sphere may be covered with a simpler insurance. Even if a general trend is to create different stand-alone cyber

policies in order to response focusing on a particular need of organizations (US Homeland Security, 2012), cyber-caused events may also be covered by general comprehensive policies, such as, for instance, physical damages due to successful attack on SCADA system are covered by traditional property insurance (US Homeland Security, 2012).

Therefore, the insurance may act as a facilitator tool in order to collect information and risk assessment (Cukier, 2005), which will enable insurers with greater information power as they may improve insurance conditions, terms and premiums. Information are so important in this market in order to ensure protection and security for critical infrastructures that information flow must be continuous based on constant observation of actual conditions, which expresses the real terms of the environment, and, moreover, information need to be shared among the most relevant stakeholders, such as competitors, government, and other institutions and agencies (US Homeland Security, 2012).

Furthermore, insurance market, in order to be the most fair and efficient, needs to have a reasonable and enough good knowledge about the expected losses and their likelihood of occurring by tracing and knowing the probability distribution of the insured events (Rowlands, Devlin, 2006). However, the probability of events theorizes the independency of events, instead in the case of CI the interrelation among events, components and infrastructures are present and strong, thus it challenges the analytics of past events in order to foreseen future ones (Rowlands, Devlin, 2006).

Even if insurance market may still present possible failures, insurance for critical infrastructure is a possible way to protect nations' capabilities to ensure to the society a future and present wellbeing. However, incentives are requested in order to boost and improve the accessibility to insurance in order to mitigate risks and costs. In order to improve economic efficiency, it is required to encourage firms in engaging the optimal level of risk mitigation (Rowlands, Devlin, 2006); it is possible by requiring in terms of insurance contract more investment. Insurance, therefore, acts as a collector of information and best practices which are shared across the industry, improving the efficiency and the protection of data, software and business. Otherwise, the

implementation of insurance in this business field may be boosted thanks to site visits and contract obligations which highlight best practices that prevent loss and mitigate the majority of risks (Rowlands, Devlin, 2006). Incentives are needed also in order to improve risk mitigation strategies by leveraging on financial incentives. In fact, insurance premiums may act as incentives, as they can be reduced if more effective prevention and protection measures are applied, therefore, in order to see reduced their premiums, critical infrastructures are more inclined to make investments focus on security and protection of their assets (Rowlands, Devlin, 2006).

However, insurance applied to CI still has challenges to be addressed, as the distribution of losses is a big and important incognita and behavioral patterns, both from CI owners and operators and from malicious attackers, are not well understood and unknown in some cases, insurance market present possible failure, because contractual terms may not describe the actual situation and the pricing mechanism may present serious inaccuracies (Rowlands, Devlin, 2006). Moreover, the strong and extended interrelations and interdependencies among critical infrastructures linked to social reliance on these providers of essential services and goods highlights the enormous gap between the losses suffered and recovered thanks to insurance and the more significant social costs of services disruptions (Rowlands, Devlin, 2006), as severe energy blackouts show and shutdowns of telecommunication demonstrate.

In conclusion, it is still important the government contribution to insurance market and critical infrastructures, where government should focus on major cyber/physical events and on helping stakeholders by assuming the role of *super partes* (US Homeland Security, 2012). Even if governmental agencies succeeded in identifying cyber threats and theirs sources, it is up to organizations to insure their operations by deciding which cyber threats address, as it is useless and inefficient to "*insure against everyone and everything*" (US Homeland Security, 2012), by implementing protection strategies which address basic cyber threats, and by relying on agencies cooperation if a complex cyber attack should occur.

5.2 IMPROVING CYBER INSURANCE

Since cyber threats are becoming always more significant to businesses and society is always more sensitive to their effects, organizations and critical infrastructures have understood the importance of sided cyber security practices with insurance mitigation capabilities. In order to avoid inefficient approaches, insurers have modelled different and evolving approaches in order to quantify risks and measure effectiveness of cyber security and risk management strategies.

Cyber insurance reflects a new approach to risk management which represents psychological and economic driven technique (Pal *et al*., 2011). Its importance is growing because the implementation of cyber insurance would produce numerous benefits, as it could increase Internet safety (Bolot, Lelarge, 2008) (Pal *et al*., 2011), then cyber insurance may change the mindset of industries that rely on cyber space for their businesses, since it is proven that risks cannot be absolutely cut off , but organizations prefer mitigating them by transferring them to insurance companies (Pal *et al*., 2011), furthermore, the implementation of cyber insurance will act as an alignment tool using economic incentives in order to align insurers and clients (Pal *et al*., 2011).

In this section, different models of insurance will be exposed in order to examine the different characteristics that are offered by insurers which tend to maximize the total outcome as the sum of clients, thanks to the mitigation offered by the insurance company, of insurers, as they collect an higher premiums and do risk less, and of society, as the improved protection may ensure the totality of users of better status of the Internet and provided services in case of CI.

5.2.1. CLASSICAL MODEL

In order to understand the advancements in progressive models that will be presented, it is useful to start with the classical model for insurance, which is described by classical expected utility model (Bolot, Lelarge, 2008), through which agents try to maximize the expected utility function. In this setting, agents are assumed to be rational and risk adverse, which plots a concave utility function (Bolot, Lelarge, 2008). By denoting with w_0 agent's initial

wealth, with π risk premium, which expresses the willingness to pay maximum amount in order to not incur in pure risk, denoted as *X* and which expresses a centered random variable with E[*X*] = 0, the equation with equals the risk premium to an amount of money paid for covering risks, which decreases the initial wealth is

$$U[w_0 - \pi] = E[U(w_o + X)] \text{ (Bolot, Lelarge, 2008)}$$

At this point, it is introduced the potential loss L which can occur P probability, for thus the agent may be obliged to pay a sum of money *m* in order to escape the risk (Bolot, Lelarge, 2008).

Therefore, the function is

$$PU\,[w_0 - L] + [1 - P]U[w_0] = U[w_0 - m], \qquad \text{with } m>PL$$

From this last equation, it is possible to calculate the amount of premium that an insurer can request in order to transfer risks, which is possible to equal to *m*, consequently

$$m = PL + \pi[P]$$

where *PL* represents the fair premium, which corresponds exactly to the expected loss and *m* expresses the maximum acceptable premium for full coverage of risk. From the insured point of view, the contract will be accepted if the cost of insurance is lower or equal to *m* (Bolot, Lelarge, 2008), whilst, for insurance company's perspective, the premium is a function of the distribution of losses, expressed in the second equation by *P* and *L* (Bolot, Lelarge, 2008). In conclusion, the classical model of insurance can be expressed by the existence of a market as a function of *U*, the utility function, *L*, potential losses and *P*, likelihood of the negative events (Bolot, Lelarge, 2008).

5.2.2. SYSTEM MODEL

According to Pal and Hui (2012), system model of cyber insurance is designed for heterogeneous network users in order to value appropriately premiums now based on user risk types. This topological approach theorized by Pal and Hui (2012) proposes a mechanism based on positive externalities caused by network users that are absorbed also by other users, and on network location of users. The model considers a monopolistic agent – insurer who provides full coverage in a compulsory insurance scenario (Pal, Hui, 2012). Clients are

network users and risk adverse, they invest in self-defense strategies until a certain level, this level is proportional to the likelihood of incurring in loss due to cyber threats and risks (Pal, Hui, 2012), and moreover, it determines the user's location within the network and user's risk type. The system is assumed to charge fines to high-risk users while providing discount to low-risk users (Pal, Hui, 2012). The communication network is a static N-node network, where the links are assumed by theorem to express externality effects of investment on node j on node i (Pal, Hui, 2012). Therefore, this model assume the role of helping a monopolistic cyber insurer in order to efficiently allocate fines or discount on insurance premiums according to risk type of users, theoretically the optimal fine or discount per user should be allocated in proportion to Bonacich or eigenvector centrality value of the user (Pal, Hui, 2012).

5.2.3. SELF-PROTECTION MODEL

The insurance applied to cyber space is proved to provide significant positive effect on network's users who face correlated and interdependent risks (Bolot, Lelarge, 2008), therefore, insurance acts as a promoter of network-wide changes improving the network status thanks to massive investments on self-protection, which in turn by developing insurance markets capabilities and products also the Internet will benefit thanks to a wider scale employment of cyber insurance (Bolot, Lelarge, 2008). According to Bolot and Lelarge (2008), security strategies involve or self-protection, which aims at reducing the likelihood of loss, or self insurance, whose objective is to reduce the magnitude of loss, consequently, intrusion detection and prevention systems are typical mechanisms of self-protection that organization implement, whilst DoS mitigation systems and traffic engineering solutions are classical tools of self insurance, also public relations act as mitigation of loss magnitude by sending astute messages to investors, by reducing the impact of cyber attacks, especially security breaches, on company stock (Bolot, Lelarge, 2008).

Bolot and Lelarge (2008) design the problem starting from optimal self-protection in no-insurance setting. It is expected that larger investments in self-protection is translated into a lower probability of loss. The researchers denote with c the cost of self protection, with $p[c]$ the likelihood of loss, and it is a

non-increasing function of c. The optimal level of self-protection, according to self-protection model (Bolot, Lelarge, 2008), is expressed b the value of c^* maximizing the equation

$$p[c]U[w_0 - L - c] + (1 - p[c])U[w_0 - c]$$

Therefore, the optimal cost is 0 or c_t.

The next evolution of this simpler model assumes an agent with a binary choice invests c or does not invest. Thanks to this evolution, insurance becomes a choice for the agent, since if the equation

$$c < (p^+ - p^-)L + \pi[p^+] - \pi[p^-] =: c_{sp}$$

does not hold, the best option for agent is to not invest in self-protection, but the choice is moved towards insurance (Bolot, Lelarge, 2008). Moreover, this last equation expresses the level of self-protection only if the cost is respecting this inequality. At this point, analyzing another equation is possible to further examine the premium and understand if insurance is the optimal strategy.

$$\vartheta < p^+L + \pi[p^+], \quad \text{where } \vartheta \text{ represents insurance premium}$$

In fact, if this equation holds, the premium results low enough to indicate that insurance is the optimal strategy for users (Bolot, Lelarge, 2008). However, premium needs to be combined with a certain level of self-protection in order to discourage moral hazard behaviors, therefore, insurers tend to tie up premiums with self-protection strategies in order to avoid moral hazard.

The more general method of cyber insurance takes into consideration heterogeneous users, who face different and various costs for self-protection, even if self-protection effects are the same (Bolot, Lelarge, 2008). The differentiation in costs will divide users in two main categories with different behavior toward insurance, since users facing low costs tend to invest in prevention and self-protection strategies, while users with high costs will not encourage in investing in self-protection. By denoting $F_n[c]$ as the fraction of users facing self-protection costs lower than c, s_j as different possible values for self-protection costs, F_n as an increasing function for each s_j by the fraction of nodes having a cost of s_j (Bolot, Lelarge, 2008), therefore c is determined as

$$\hat{c} = min\left\{s_{j-1}, F^n[s_{j-1}] < \frac{k^n[s_j]}{n}\right\}$$

So, this equation expresses the relation between insurance and self-protection as insurance increases the adoptability of self-protection investments for any user in the communication network (Bolot, Lelarge, 2008).

In conclusion, the aim of this model is to show to insurers a compromise between insurance premium and self-protection strategies, that do not exclude or equal the effects and benefits of insurance, but it needs to implement the optimal union of self-protection and insurance, in order to avoid and decrease one of the most annoying problems of insurance, *i.e.* moral hazard. The authors, however, states that numerous difficulties and challenges are still in place in cyber insurance field, as quantifying the optimal premium since risks threaten intangible assets, the damages might be noticeable in the long run, because risks can easily and rapidly change and because the evaluation of insurability and the level of self-protection of customers is still representing a complex and time-intensive tasks (Bolot, Lelarge, 2008).

5.2.4. INTERDEPENDENT SYSTEM MODEL

According to Ogut *et al.*, (2004), cyber insurance is a function of interdependent risks and IT security, showing that interdependency of IT security risks between firms significantly affects insurance coverage and firms' incentives to invest in cyber security. The authors find out that interdependency impact the decisions of firms about cyber security and cyber insurance, as a high degree of interdependency decreases IT security investments and cyber insurance purchasing under the optimal social level. Cyber insurance market will be efficient when the development will ensure a decrease in insurance prices (Ogut *et al.*, 2004), since it appears that cyber insurance is less requested by firms due also to under-developed insurance market, which does not ensure clients and stakeholders (Ogut *et al.*, 2004). Therefore, it is important, in order to induce firms in investing cyber security and cyber insurance, to introduce punishment mechanisms, such as fines, and cooperation mechanisms, such as information sharing, in this way it may be possible to mitigate the negative effects due to interdependency and to boost investments in order to reach the social optima level (Ogut *et al.*, 2004).

Cyber interdependencies represent a serious risk for security, since, first of all, computers are linked through the Internet, then, due to logical interdependency, the standardization of platforms facilitate cyber hackers in breaching security and data. Consequently, due to these risks of interdependency, firms should be more inclined in investing in cyber insurance in order to hedge and mitigate these risks (Ogut *et al*., 2004).

The results of this model bring to a corollary extended to n firms, which states firstly that, at the increasing of interdependency, investments in cyber security and insurance decrease or stay equal, these conditions can be expressed by $\frac{\delta z}{\delta q} < 0$ and $\frac{\delta I}{\delta q} \leq 0$, z denotes the amount of investment in self-protection, I stands for investment in cyber insurance, while q denotes the probability that a firm n will be breached given that a firm N has been breached, therefore q expresses the degree of interdependency between IT security of n firms (Ogut *et al*., 2004). Secondly, the corollary expresses that as the number of firms increase, cyber security investment level for individual firms and insurance coverage decrease or remain stable (Ogut *et al*., 2004), since $\frac{\delta z}{\delta n} < 0$ and $\frac{\delta I}{\delta n} \leq 0$, with n expressing the number of firms.

The interesting result of Ogut *et al* (2004) is that the maturity of the cyber insurance market does not affect directly the price of insurance, since a more mature insurance market would result in a decreasing of self-protection investments which increase the insurer's risks, which in turns worsen the conditions and costs of insurance (Ogut *et al*., 2004).

5.2.5. AEGIS MODEL

This model has been presented by Pal et al. in 2011, answering the needs of insurance market and its clients since the AEGIS model is particularly suited when users cannot discriminate between types of losses and risks that may be due to cyber attacks attempting security or to non-security related failure (Pal et al., 2011), such as hardware failures due to reliability lack or bluffer overflow. This model, therefore, takes in consideration a possible solution for cyber insurance in the case that users face risks of different sources, from security failures and non-security malfunctions (Pal et al. in 2011), by introducing, further, the extra dimension of uninsurable risks.

The assumption of the model is that users accept a positive fraction of loss recovery while transferring the remaining loss burden on cyber insurer. Moreover, AEGIS model suits only if cyber insurance purchasing is mandatory, consequently, risk adverse users would prefer AEGIS insurance over traditional cyber insurance; the results of the study show a peculiarity of this model, since an increase or decrease of the AEGIS premium nay not always lead to a decrease or increase in user demand (Pal et al., 2011). The benefit of the model is incentivizing users' personal responsibility of protecting their own systems (Pal et al., 2011).

The model is based on the concept of co-insurance, as designed in the general insurance literature (Pal et al., 2011), and it states that the final wealth reached with AEGIS model is

$$W = w_0 + v - L_s - L_{ns} + \vartheta[I(L_s) - P]$$

with L denoting the loss value; $L - d$, with $d > 0$, is the insurance coverage; ϑ is the part of risk transferred to insurer, while $1 - \vartheta$ is the risk client allows to bear, where ϑ , level of cyber insurance liability of user, is a value fixed and decided between user and insurer (Pal et al., 2011); where W is a variable standing for user's final wealth; $w_0 + v$ represents the initial wealth, with v as the value of the object which suffers loss due to security or non-security incidents (Pal et al., 2011); L_s is denoting random variable of security-attack loss, while L_{ns} is random variable expressing losses due to non-security failures, both these values lie in the interval $[0; v]$; $I(L_s)$ is a cyber insurance function fixing the amount of coverage that has to be provided if a security-related loss occurs, where $0 \leq I(L_s) \leq L_s$.

AEGIS model has been built on idealistic assumptions since the model works under conditions of mandatory insurance purchasing, in an existent market and where information asymmetry is absent (Pal et al., 2011).

5.2.6. COPULA PRICING FRAMEWORK

Thanks to Herath and Herath (2006) (2011), it is possible to price cyber insurance products by using copula methodology in order to model dependent risks through an actuarial approach, this methodology focuses on risk transference in order to minimize financial losses due to security breaches and

to integrate security strategies to mitigate residual risks after cyber security investments (Herath, Herath, 2006). Copulas are mechanisms that allow to study and analyze dependence between random variables, copula framework effectively forecasts the value of losses due to cyber attacks and allows a proper pricing of cyber insurance (Herath, Herath, 2006). This framework considers, in order to assess risk posture and to estimate losses, "computer product diversity, lost productivity, lost revenue, and clean up cost" (Herath, Herath, 2006). The benefit of copula pricing framework is providing a deeper awareness of cyber security which causes a wider collection of data about cyber crimes and security breaches for negotiating lower premiums (Herath, Herath, 2006).

In order to price premiums, the model starts identifying the probability and magnitude of potential failures through a loss function

$$L = s_1 a_1 f_1 + s_2 a_2 f_2 + \cdots + s_n a_n f_n, \qquad \text{where } a_1 + a_2 + \cdots + a_n = 1$$

where a_n denotes the fraction of computers of type n, f_n values the dollar impact for computer and s_n which represents the security posture coefficient (Herath, Herath, 2006).

The cost of cyber insurance covering first party liability is

$$C = \omega e^{-rT} P$$

where ω is a binary variable, which is equal to one if the adverse event occurs or it is zero otherwise, T is the lapse of time until security incident, r is discount rate and P represents the amount paid by insurer if the event happens (Herath, Herath, 2011). From this equation, it is possible to derivate the equation for determining the net premium, which does not include costs and profits faced by insurer.

$$E(C) = \bar{\omega} E(e^{-rT}) E(P), \qquad \text{where } \bar{\omega} = E(\bar{\omega}) = Prob(\omega = 1)$$

In order to price premium actually charged by insurance companies it needs to add a mark-up that covers expenses and profits (Herath, Herath, 2011).

5.2.7. CORRELATION MODEL

This model highlights the importance and the challenge of correlation and dependencies in cyber space, which link computers within and outside the firms' boundaries through the Internet, exposing IT systems to numerous

attacks and security breaches (Bohme, Kataria, 2006). Because of homogeneity and interdependencies, failures in IT system are highly correlated, even if classes of cyber risks have different correlation properties that affect IT systems (Bohme, Kataria, 2006). However, single firms take care of correlated cyber incidents that lay within their own networks (Bohme, Kataria, 2006), and, consequently, they measure their efforts according to their individual benefits, while, insurers, by having a large risk portfolio, are concerned about global correlation and the influences of single internal correlations on other firms and the industry, since the global correlation is found to affect premium charged (Bohme, Kataria, 2006). The model is structured on two tiers, where the first tier represents cyber risk correlation within firm, meaning correlated failures of multiple systems on internal network (Bohme, Kataria, 2006), while the second tier is risk correlation at global level across independent firms collected in insurers' portfolio (Bohme, Kataria, 2006).

Figure 5.2 : Classes of cyber risk correlation

	Global correlation ρ_G	
Internal correlation ρ_I	Low	High
High	Insider attack	Worms and viruses
Low	Hardware failure	Spyware/phishing

Source : Bohme R., Kataria G., Models and Measures for Correlation in Cyber-Insurance, Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK, June 2006

In figure 5.2, it is possible to immediately have an idea about what kind of correlation faces firms and insurers, and to understand the challenges and danger of high cyber risk correlation (Bohme, Kataria, 2006). Analyzing internal correlation, failure due to hardware damages does not influence other IT system machines inside or outside the firms, nor is influenced by other outside or inside failures (Bohme, Kataria, 2006); therefore hardware failures represent a low intra-firm correlation and a low global correlation. While cyber attacks coming from inside the firm represent a real challenge for the firm, showing a low global correlation but a high internal correlation, since internal attackers can effectively affect computers within only-administrative domain, not compromising others outside this domain (Schultz, 2002). On the other

side, a high global correlation is exhibited by software attacks, such as phishing or spyware attacks, with a low internal correlation since careless employees, who may open and forward a phishing email or installing inadvertently a vector of attacks for infecting and compromising cyber systems, are few and spread in every firms (Bohme, Kataria, 2006). While, worms and viruses represent a serious risks for firms, since they have high global and internal correlation.

By analyzing these correlations, insurers can understand their effects on the overall market and on premiums (Bohme, Kataria, 2006).

The correlation model is analyzed from supply and demand side of cyber insurance and the equilibrium conditions with k-firm in risk portfolio. From supply side, losses and claims are correlated to global correlation factors. On demand side, it is important to analyze the effectiveness and efficiency of firms' information systems, since, due to different dependence on information, an information failure can limit business functions and represents a sever loss for firms (Bohme, Kataria, 2006).

Firms' willingness to pay premiums is marginally greater than facing expected loss, in competitive insurance market (Bohme, Kataria, 2006). However, in a reality setting, because of cyber risk correlation structure, premiums do not always represent economic reasons, as they depend on expected costs faced by insurance companies for settling claims in a given period (Bohme, Kataria, 2006)

$$C = E(L) + A + i \cdot c$$

where C represents insurer's expenditures, $E(L)$is expected loss, with L as a random variable; A expresses sum of all administrative costs; c is safety capital required in order to settle claims, if L is $\varepsilon -$ worst case, with ε being the likelihood of ruin for insurers; i represents interest rate for safety capital, which reflects associated risk of business (Bohme, Kataria, 2006). This model states the importance of insurance profit and competitiveness of insurance market, which may improve premiums conditions.

From this model, it is possible to address changes to be undertaken in order to improve insurance market, by operating on technical, managerial and policy side. In fact, on technical side, it is required a stronger emphasis and focus on platform diversity, in order to model countermeasures against internal and global correlation, by improving reliability and by increasing redundancy

(Bohme, Kataria, 2006). Improving managerial approach acts on limiting standardization of business practices, such as outsourcing, which create hidden liabilities difficult to be addressed with risk management strategies (Bohme, Kataria, 2006). On the other side, policy makers are required to operate a multi-angular approach, thanks to indirect control of the market due to competition policy, or by making cyber insurance mandatory for firms, or by reducing regulatory burden, making insurance market more appealing to firms (Bohme, Kataria, 2006).

5.3 EVOLUTION AND CHALLENGES OF CYBER INSURANCE MARKET

As shown in 5.2, cyber insurance market, thanks to its novelty, leaves large room for adapting its conditions and terms to changing needs of firms and users in order to propose new models of insurance according to firms' budget and risks. Moreover, cyber insurance market is in flux, with higher competitiveness in this market, providing great opportunity for firms' risk managers and proving that insurance and consulting are important practices in businesses (Perspectives on Insurance Recovery, 2012).

Today's cyber insurance market is characterized by an augmented demand for breach notification insurance, since the most noticed and clamorous cyber related losses are due to data and security breaches (US Homeland Security, 2012). Nowadays, trend of firms plots an unwillingness of paying for cyber security insurance, as the common mindset is not focused on preventing risks but it is preferred to pay as a remedy to cyber attacks or security breaches (US Homeland Security, 2012). In order to improve the conditions of the demand side, showing an old-style mentality, it needs to address better education of firms and businesses about the importance of cyber threats and risk posture of the firms (US Homeland Security, 2012). Even if modern policies are fixed and predetermined, there is a growing trend of developing custom-drafted policies (US Homeland Security, 2012) in order to offer a wider and more focused protection to clients. However, this offer needs a background analysis of data shared by their clients (US Homeland Security, 2012) and it requires, therefore, that firms do understand the value of their data and the real cyber risks and threats in order to take, at first place, the adequate precautions and strategies to be taken against these cyber threats (Buckler, 2005).

US cyber insurance market is expected to grow, as it shows estimated figures of total premium spend around $500 million, which enlarges insurance product development and increases the risk exposure capacity (Airmic technical, 2012). While increasing in European, Australian and Middle East markets is expected, the real and fast expansion of markets relies on legislative development and its impact on firms' cyber security strategies (Buckler, 2005). In fact, a change in

legislation can affect other markets and firms in the decision of investing or not in cyber insurance.

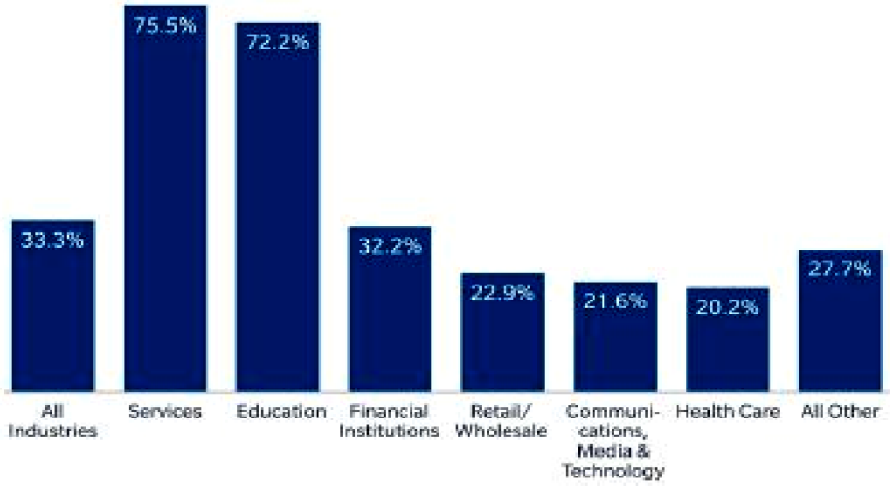
A first big change is happening in 2014 when the European Union is starting imposing fines on companies that suffer significant data and information breaches, this manoeuvre may represent a total up to 2% of business's global revenue. Consequent to this significant penalty, firms would be more inclined to focus on cyber security and strategies in order to prevent and mitigate possible cyber threats and more interested on cyber insurance (US Homeland Security, 2012). The benefit desired by EU is to incentivize businesses in prioritizing cyber security strategies by increasing focus and cyber security measures (US Homeland Security, 2012). In fact, firms are not inclined to report cyber-attacks due to reputational damages, and therefore, the consequent lack of data about cyber attacks worsens the conditions of insurance market in providing suitable covers.

According to Ponemon Institute (2013), a stronger security posture assumed by the company may follow purchase of cyber insurance, as stated by 62% of survey respondents believing that company is better prepared to face cyber threats, this approach is considered an important step in risk management strategies by 55% of respondents. However, there are still a non-insignificant percentage of firms, 30%, that do not have interests in cyber insurance, since they are discouraged due to price and too much exclusion in today's insurance policies that inhibit purchasing because of restriction and uninsurable risks (Ponemon Institute, 2013). On the other side, cyber insurance market satisfies 44% of respondents, who are likely to recommend their insurance company to colleagues, moreover, the satisfaction seems to be directly related to time policy has been held (Ponemon Institute, 2013).

The cyber insurance market has room to grow since majority of companies are planning to underwrite cyber policies, because firms become more interested in cyber security after cyber-related incidents. The desire and need of cyber insurance augment with the perception about financial exposure to security breaches and it is related to estimated impact on firms' image and financial position (Ponemon Institute, 2013). US cyber insurance market records growing percentage of underwriting of policies, with differences in industries

related to cyber security postures and cyber threats faced by different firms, as it is possible to notice in figure 5.3.

Figure 5.3 : Percent increase of cyber insurance in US market in 2012



Source : Marsh, Cyber Risk: Trends And Solutions, 2013

Therefore, cyber insurance has the power to improve information about security, since it requires a wide collection of data about cyber threats and cyber attacks; at the same way, cyber insurance can affect positively security decisions and the overall network environment, spreading the adoption of these mitigation strategies. In fact, cyber insurance may change in the medium run insurance market structure and the behaviour of technology manufacturers (Bohme, Schwartz, 2010).

In order to improve and boost the cyber insurance market, possible recommendation made by ENISA for cyber insurance market in Europe can effectively help the growth of cyber insurance (US Homeland Security, 2012), hence, ENISA recommends four main points that, if implemented throughout the industry, may improve the overall well-being of society. The first point is addressing challenges by surveying private companies, in order to determine knowledge about cyber risks and insured losses and other issues related to insurance market (US Homeland Security, 2012). This point is essential since information and firsthand data are primary steps in developing effective cyber security and, above all, cyber insurance policies. Secondly, it is suggested to explore the possibility for harmed companies of initiating collective actions

against service providers that do not adopt sufficient or ineffective cyber security measures (US Homeland Security, 2012). This step needs further analysis to be assessed if it has positive effects on encouraging better risk management practices and on making more robust cyber insurance market. Moreover, third point states that the adoption of frameworks aiming at determining a fair value of companies' information is essential since it improves decision making process about purchasing insurance products to mitigate and transferring cyber risks (US Homeland Security, 2012). Forth step is a suggestion about the role of government, since it may assume the role of last resort insurer; in fact, government can address two main challenging areas, information sharing and reinsurance. However, information sharing, even if it represents a good practice in order to collect at a higher level all those information about cyber threats and risks, which help in suiting insurance policies, is implemented through numerous federal agencies, worsening the situation and practicability of sharing information at national level (US Homeland Security, 2012); therefore, companies require that government defines and structures its agenda and agencies' agenda. About government's role of reinsurance, it could be impracticable and unlikely to assume this role, especially, towards small and medium companies that are not part of critical infrastructures (US Homeland Security, 2012); moreover, stakeholders believe that last resort insurer role of government should be assumed only if in extraordinary events, such as a "cyber tsunami" (US Homeland Security, 2012) or because of intensive and significant public pressure towards increased security reached through cyber insurance (US Homeland Security, 2012).

In US, in 2011, SEC issued a "Corporate Finance Disclosure Guidance: Topic No. 2 – Cyber security", which requires disclosure of information about cyber attacks to publicly traded companies' shareholders, and it needs to disclose risk factors related to potential cyber incident (Rosen *et al*., 2014). However, this guidance does not require or encourage mandatory cyber insurance, but it assumes that firms implementing cyber insurance would have lower risk factor for cyber security (Rosen *et al*., 2014). In 2013, thanks to Executive Order 13636, national focus is moved towards critical infrastructure cyber security, requiring to numerous industries, such as chemical, transportation, financial and electricity industries, data breach notification. Even if these legislative

developments represent a stronger involvement of US government, stakeholders and political pressure is asking for greater Federal regulatory actions and efforts, since data breaches and cyber security become first public focus due to Snowden and WikiLeaks issues that show the weakness of cyber security (Rosen *et al*., 2014).

Cyber insurance has to address challenges in order to improve and boost its adoption towards firms and industries. In fact, an increased adoption of cyber insurance is proved to improve the Internet conditions for the majority of users, even those that do not purchase cyber insurance (Lelarge, Bolot, 2009). However, this overall benefit needs to discourage selfish behaviours, which increase moral hazard and free riding episodes, as firms tend to limit their investments according to their minimum security. Another challenge is clear legislation which may address proper and adequate investments of principal stakeholders toward cyber security by purchasing insurance. Moreover, a more dynamic insurance market would result in more convenient conditions of cyber insurance, by covering more damages for a lower and fair premium, which in turn would increase clients' pool attracted by suitable terms and prices.

As cyber risks increase and change, at the same time insurance market is adapting and changing rapidly by developing new products in order to meet demand' side needs (Airmic technical, 2012). A future step for insurance market would be to be focused on economics of cyber security, therefore analyzing companies' investment decisions, cyber risks management tools and outsourcing services which may increase the exposure to cyber threats (US Homeland Security, 2012).

Cyber insurance market, therefore, is essential a vital presence for companies that want to transfer cyber risks to third parties and it will have a larger role for industries as soon as governments will clarify and reason cyber security investments.

CONCLUSIONS

The title of this dissertation, *Critical Attacks : How economy could be saved by cyber insurance*, is supposed to group principal challenges that need to be addressed, since their development has been neglected under numerous point of approach. The principal hypothesis from where this thesis moves forward is that cyber insurance can effectively be a vital tool and strategy for firms, in particular for critical infrastructures owners and operators, in order to mitigate all those risks that cannot be covered and absorbed by cyber security strategies implemented by companies. Therefore, cyber insurance, thanks to a future wider adoption, could improve technology security (higher security level implemented), economy (cyber insurance market has a tangible prospective of growth in many regional markets and relevant total premium to be collected), and society (cyber threats are tangibly affecting everyday life and business routine which passes on "passive" users negative effects and damages).
Indeed, the major objective of the dissertation is to highlight the significant role of critical infrastructures and encourage cyber security with more than one approach and strategy. As seen, critical infrastructures are so important for society that a possible failure of one of these infrastructures could imply financial losses and critical damages to the Social structure.

Critical infrastructures, indeed, represent the backbone of modern society, as they become more and more important for civilized economies and also developing countries' economies. Thanks to a deep analysis of their definition, since it affects further considerations, critical infrastructures are demodulated in order to identify those whose incapability or destruction would have a debilitating impact on the defence or economic security of the nation (in Moteff, Parfomak, 2004). Another sign of criticality is the strong dependency on other infrastructures and thus strong interdependency (Hammerli, Renda, 2010); consequently, the interdependency and importance of these infrastructure are the core for the economy, government and social life, therefore there are infrastructures considered critical, since their malfunctioning and failures can bring a general disturbance or, worse, a loss of investments, efficiency and life comfort.

Singularly, nations have listed different critical infrastructures depending on national interests and weaknesses, even if there are common industries that are controlled by the majority of nations, such as electric power supply, water supply, banking and finance, defence, food, public health, telecommunications and transportation. Their existence is woven into society's habits; therefore they are under the spotlight of governments and policy attention. It is essential that critical infrastructures are robust, reliable and resilient, able to face possible risks, coming from nature or human error or attack. Several new technology-based infrastructures have been created over the last century and half (Goodman *et al.*, 2003), their development and intensive usage characterize modern society and determine its vulnerabilities.

In fact, due to the associative network, by which new nodes are added to already existing networks through other selected nodes, the majority of the critical infrastructures have not been designed to be part of an integrated system, but they have been just evolved gradually over time to accomplish required tasks, thus exposing the entire system to targeted attacks and failures that might induce risks and damages to other interconnected systems (Gheorghe *et al*., 2007).

Moreover, critical infrastructures are such a complex issues because they are vital and ubiquitous, therefore their lack of capacity or even their destruction affects not only the security and social issues of one nation, but it has devastating cascade effects across national borders, causing shock transmissions across borders and across numerous infrastructures, which determine the impossibility to consider and analyse a single-standing infrastructure detached from the environment or other infrastructures.

Since it is possible to recognize the importance given to critical infrastructures by policymakers and economists, economic and political aspects of critical infrastructures make it difficult to measure their advances, since an improvement in either side would provoke infinite effects, which could be positive or not, in many others fields and sectors due to deep and hidden interdependencies.

It highlights that strong reliance on critical infrastructures must be protected by ensuring a sustainable partnership among private and public sectors in order to address effective improvements in defense and resiliency, by creating

databases. Mapping and understanding the real conditions of critical infrastructures is the objective of databases, in order to create a more integrated management of these systems (ICE, 2009), in fact, it should be easier to improve accounting systems, enabling them to recognise precise costs and current value of infrastructures. By doing this, government has to carries out cost/benefit analysis of infrastructures, including building and maintenance costs, and comparing them to the cost to Society, environment and economics if they were to fail.

Since physical parts of these networks have to undergo to alarming range of threats coming from nature, (such as earthquakes, extreme winds, floods, tsunamis, and wildfires), but also due to terrorist acts, design faults, aging materials and inadequate maintenance. Maintenance itself is a key aspect against failure, but it is also the aspect less assessed by investors, the constant decline of the resilience of the systems, increases the probability of severe failures.

Failure of major infrastructure could provoke catastrophic effects; indeed the failure of these significant systems can cause environmental damages, important cost to the economy and possible threats to life. The actions to be undertaken in order to decrease the likelihood of failures is to adequately maintain and protect critical infrastructures and to build reserve capacity, useful during emergency actions; it is essential for this purpose to better integrate private sectors, since they can easily and better assess systems status and address proper protection, due to first-hand information and data (Brömmelhörster *et al*., 2004). Therefore, serious protection issues have to not be just limited to engineering design systems, but need to embrace topic of legacy systems, the difficulty to understand strategic threats, the need for training and information sharing. In order to face properly critical infrastructure protection (CIP), it must be acknowledged numerous challenges that, if addressed, will improve security. First of all, it has been noticed a limited pool of resources available in order to address security problems, that could increase risks and inhibit businesses. Then, the lack of sharing news about threats and incident among government and private actors can increase the risk of attacks because there is a sense of unpreparedness among actors.

This is also the result of difficultness of establishing effective partnerships between government and businesses. Moreover, it results in chaos and inefficiencies created by poor coordination among public agencies. Furthermore, the increasing sophistication of tools and methods used by hackers worsens the speed of response and its effectiveness, requiring high level of cyber security, in order to be prepared for cyber-attacks.

In order to give proper considerations, the dissertation goes on analysing Critical Information Infrastructures (CII), which are the base of many other critical sectors, linked with strong interdependencies and nebulous boundaries as Internet and telecommunications technologies (ICT) improve and enter daily life with numerous and different applications. These CII are defined as "*any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video"* (US Department of Homeland Security, 2012), these infrastructures are essential and vital to the functioning of other critical infrastructures and the nation which infrastructures are incapacitated or damaged, would be affected by strong and unbearable impacts on security, economy, public health and safety.

In fact, Critical Information Infrastructures are more sensitive to external attacks and technological vulnerabilities, which can be easily exploited by malicious attackers. Internet is by design open and exposed to threats, but at the same time it leaves room for improvements and to reduce vulnerable points of access, in order to improve and boost its resilience and robustness and, consequently, of all the other critical infrastructures which rely upon it. The risks of man-made attacks, since cyber-attacks and cyber warfare are real issues which reach an unpredicted level of sophistication of attacks, hide behind profit or political causes, and failures do conjunct with the high degree of interdependency of ICT and other critical infrastructures and with cross-borders interconnections (EU Commission, 2009).

However, there is a lack of knowledge of the risks and threats that CIIs face, which, consequently, decreases the effectiveness of security plans. Moreover, the interdependencies (OECD, 2002) on which critical infrastructures rely on, among ICT and critical infrastructures, are nowadays essential and vital also in

government services, SMEs and individual users, which use in everyday operations cloud computing services and other Internet services. This importance is due to the increased capability of delivering information and instructions to and from all the critical infrastructures, which makes critical to Society the presence of efficient ICTs (Clemente, 2013), giving more importance to the Internet and further highlighting the severe cyber threats.
As a matter of fact, this massive approach to ICTs, due to the increasing recourse to Internet and its application, makes critical all the infrastructures involved and which have strong interdependencies with. The most challenging topics are data protection, infrastructure and architecture security, protection from cyber-attacks and resilience and robustness against natural disasters. All these require massive investment on security and protection, making all CIIs resilient to any sort of failures.

As WikiLeaks has proven, the security and protection of sensitive information and data becomes a priority for organizations, which try to construct valid models that could help business to deal efficiently with everyday operations and processes. Thus attacks as computer security breaches, confidentiality and integrity, are carried in an increasing number on various targets, from business to governments (Colwill et al., 2001)
Therefore, models and management strategies would be useful and essential for business in order to handle carefully these key assets. In this vulnerable setting, information assurance is fundamental in order to provide appropriate levels of confidence over system security and critical assets. In fact, information assurance represents "*operations undertaken to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation*" (IAAC, 2000), therefore, it incorporates a holistic approach, including scientific, technical and managerial capabilities, in order to protect and defend information systems. However, in order to effectively assure information, it is not enough to apply IA models, but organizations have the duty to implement a rounded-approach to risks, in particular to knowledge and IT risks, and to management of information flows.

Since ICT represents the pivot of the "*world system*" (Antinori, 2008) as constitutes the background for CI and in particular CII, cyberspace and computers become the key platform for the complexities of human and economic flows, by running businesses, connecting people and providing government services. However, the higher is the interconnections and interdependences, the higher is the reliance on the Internet which creates opportunities to be exploited by cyber attackers and increases the shock wave and damages caused by the attack. Because of these reasons, cyber attacks are considered by US National Intelligence as the most pressing threat to US Security, ahead of Islamist terrorism, although the likelihood of an event is admitted to be very low (Dyer, 2011). The same way as terrorism and other national threats, cybercrime is associated with different and numerous losses, estimated to be approximately at worldwide level US$1 trillion (Ponemon Institute, 2013), and costs derived by enhancing better passive cyber defense and in some cases planning offensive cyber actions.

Cybercrime acts in order to exploit three outcome effects, fear factor, which is aimed at creating the maximum fear in people by striking IT installations and especially critical infrastructures; spectacular factor, expressed in massive direct losses or in colossal media coverage, which makes the actual damage insignificant for cyber crooks; vulnerability factors, through which demonstrate the weakness of organizations by causing denial of service or by vandalizing organizations' web pages.

However, the magnitude and impact of cybercrime is challenging to quantify, since cyber attacks are not always detected or reported to authorities (Càrdenas *et al*., 2010), moreover there is no standard method for cost measurement in relation with the analysis of likelihood of cybercrime. Furthermore, the reluctance of organizations to disclose information on security breaches is explained because of the negative impact (Càrdenas *et al*., 2010) that these news cause to businesses, such as a negative financial market impact due to security breach announcement, now perceived more risky; then there are reputation and brand damages, which generate confidence loss in consumers. Litigation are feared as a disadvantage for the complete disclosure of security breaches, as investors or other stakeholder may seek through law enforcement recovery of damages; moreover, disclosing may highlight a non-adherence of

managers to regulations, therefore arising liability concerns; reporting signals to other potential attackers that information systems of organization is vulnerable and easily exploitable; moreover, IT personnel may act egoistically and fear for their job security trying to hide the breach.

In the dissertation, it is given a full description of three of the most important and concerning aspects of the dark side of the Internet, cyber attacks, cyber warfare and cyber terrorism, as these aspects represent the evolution of cybercrime, which comes alongside with technology advancements, and reflect the different intentions of attackers. Moreover, a clear and net distinction between these terms is useful when a strategy for security and protection need to be designed, and it needs to take into account the different consequences and targets. In fact, protection has to be tailored in order to respond actively to different characteristics of these cyber threats that change in outcome factors, among fear, spectacular or vulnerability factors, which reflect the intention of cyber crooks, and characteristics that differ in final damages, that could be physical, psychological or financial.

Cyber threats require awareness and improved security practices, that need to be shared and known by any user. Therefore, it should be addressed the creation and implementation of robust culture of cyber security (Cornish *et al*., 2011) in order to create an homogenous basis of security which is shared by the majority of users. In fact, technology has to be supported with cultural and human factors, which must be trained, improved and empowered in order to offer a better protection of sensitive data and resources, which constitute a competitive advantage for organizations. Even if there is no uniform or shared approach to cyber security, few national or private organizations related to cyber security aim at providing standards and guidelines for organizations. Therefore, it is possible to trace down few general guidelines which enables every organization and users to secure and protect their IT systems and information. In general terms, good practices are required, as they represent the level of cyber dependencies awareness, they reflect the knowledge and understanding of the supply chain and the long-term perspective the

organization assumes in order to monitor risks and be prepared for respond to threats (Cornish *et al.*, 2011).

However, a growing concern is the protection and security of control systems, like SCADA, against malicious attacks, since cyber-attacks need to be more elaborated in order to be able to manipulate and damage critical infrastructures, and therefore such attacks require time, efforts and expertise of considerable extent (Geers, 2009). The protection of these systems could be incentivized by cooperation between asset owners and vendors, in order to boost the implementation of best security practices (Càrdenas *et al.*, 2009). The more adopted ongoing strategy is to focus on reliability, ensured against random faults that SCADA may meet. However, a more comprehensive security strategy includes the importance of detection and response to attacks, by monitoring physical system and checking detectable anomalies, which can indicate under-way attacks (Càrdenas *et al.*, 2009).

The conclusion of this complex discussion about cyber security ends in stating that, in order to prevent or mitigate damages of cyber-attacks, security frameworks help managers and strategists to construct and apply a suitable and tailored cyber security which is consistent with factors, such as economic, political and cultural. Implementing basic principles at IT system infrastructure, as dictated by Dr. Amoroso (2011), may ensure an efficient cyber security for the most technological structures, such as critical infrastructures which need a special and more focused security and defense in order to avoid severe damages for society.

Consequently, the organization which runs critical infrastructure by employing an efficient CIP and CIIP, it has assured the information supply chain and secured its cyber infrastructures against cyber-crime, ensuring stakeholders and insurance operators that the organization has low likelihood of suffering severe damages provoked by cyber criminals. By implementing these protection and security strategies, an organization is reassuring and stating its risk appetite in order to successful underwrite a cyber-insurance which helps to mitigate unexpected or residual risks and damages, which are unprotected through all the security actions undertaken.

Therefore, cyber security procedures, that have been shown throughout this dissertation, such as information assurance and cyber security strategies, need to be sided with other deterrents as cyber security strategies cannot prevent all potential attacks, which are always more aggressive and resourceful.
Since there is a growing dependency on technology and an increased threat of unauthorized access to data and information, there is also a response of insurance market to these challenges, backed by an increased awareness and knowledge of corporations about cyber risks and exposure (Airmic technical, 2012), consequently, the potentiality of insurance results significant for organizations as a control mechanism.

The thesis, at this point, reaches its objective to expose the benefits of implementing cyber insurance for firms, and especially, for critical infrastructures and CII.
Even if insurance market may still present possible failures, insurance for critical infrastructure is a possible way to protect nations' capabilities to ensure society future and present wellbeing. Therefore, the insurance may act as a facilitator tool in order to collect information and risk assessment (Cukier, 2005), which will enable insurers with greater information power as they may improve insurance conditions, terms and premiums. Information are so important in this market, in order to ensure protection and security for critical infrastructures, that information flow must be continuous based on constant observation of actual conditions, which expresses the real terms of the environment, and, moreover, information need to be shared among the most relevant stakeholders, such as competitors, government, and other institutions and agencies (US Homeland Security, 2012). Insurance, therefore, acts as a collector of information and best practices which are shared across the industry, improving the efficiency and the protection of data, software and business.
Insurance market in order to be the most fair and efficient, needs to have a reasonable and good enough knowledge about the expected losses and their likelihood of occurring by tracing and knowing the probability distribution of the insured events (Rowlands, Devlin, 2006). However, because of non-independency of events, since the case of CI the interrelation among events,

components and infrastructures are present and strong, the analytics of past events in order to foreseen future ones is challenged and complex (Rowlands, Devlin, 2006).
A benefit of cyber insurance implementation is that cyber insurance has the power to improve information about security, since it requires a wide collection of data about cyber threats and cyber-attacks; at the same way, cyber insurance can affect positively security decisions and the overall network environment, spreading the adoption of these mitigation strategies.

Incentives are requested and needed in order to boost and improve the accessibility to insurance in order to mitigate risks and costs. In order to improve economic efficiency, it is required to encourage firms in engaging the optimal level of risk mitigation (Rowlands, Devlin, 2006); it is possible by requiring as terms of insurance contract more investment. It is still important the government contribution to insurance market and critical infrastructures, where government should focus on major cyber/physical events and on helping stakeholders by assuming the role of *super partes* (US Homeland Security, 2012). Even if governmental agencies succeeded in identifying cyber threats and theirs sources, it is up to organizations to insure their operations by deciding which cyber threats address, as it is useless and inefficient to "*insure against everyone and everything*" (US Homeland Security, 2012), by implementing protection strategies which address basic cyber threats, and by relying on agencies cooperation if a complex cyber attack should occur.
Cyber insurance has still to address challenges in order to improve and boost its adoption towards firms and industries. In fact, an increased adoption of cyber insurance is proved to improve the Internet conditions for the majority of users, even those that do not purchase cyber insurance (Lelarge, Bolot, 2009), to improve cyber security and to reassure stakeholders.

In conclusion, it is possible to state that, as this thesis tried to prove and explain, cyber insurance market is essential and a vital presence for companies that want to transfer cyber risks to third parties and it will have a larger role for industries as soon as governments will clarify and reason cyber security investments. In special way for critical infrastructures, cyber insurance

represents an effective and efficient tool in order to encourage owners and operators to implement improved cyber security strategies and it reassures stakeholders of the reliability and resilience of these backbone structures, which are assumed to continue providing their services for the sake of the society well-being.

REFERENCES

About Critical Infrastructure, Public Safety Canada, [www.ps-sp.gc.ca]

Airmic technical, Airmic Review of Recent Developments in the Cyber Insurance Market & commentary on the increased availability of cyber insurance products, 2012

Alberts C., Ellison R.J., Woody C., Cyber Assurance, CERT, 2009

American Petroleum Institute and the National Petrochemical & Refiners Association, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, May 2003

Amoroso E.G., Cyber Attacks: Protecting National Infrastructure, Elsevier, 2011

An Emergency Management Framework for Canada, Ministers responsible for Emergency Management, 2011, [http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/mrgnc-mngmnt-frmwrk-eng.pdf]

Anderson B., Anderson B., Seven Deadliest USB Attacks, Syngress, 2010

Anderson R., Fuloria S., Security economics and critical national infrastructure, The Eight Workshop on the Economics of Information Security, 2009

Anderson R.D., Insurance Coverage for Cyber Attacks, issue of The Insurance Coverage Law Bulletin , Vol. 12, No. 4, June 2013

Angelini M., *et al*., 2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness, Research Centre of Cyber Intelligence and Information Security "Sapienza" Università di Roma, December 2013, Casa Editrice Univarsità La Sapienza, [http://www.dis.uniroma1.it/~cis/media/CIS%20Resources/2013CIS-Report.pdf]

Antinori A., Information Communication Technology & Crime: the Future of Criminology, Rivista di Criminologia, Vittimologia e Sicurezza Vol. II - N. 3 , Settembre-Dicembre 2008

Antinori A., Sviluppo nell'ambito nazionale del concetto di information assurance relativo alla protezione delle informazioni nella loro globalità, CEMISS, 2011

Armerding T., The 15 Worst Data Security Breaches of the 21st Century, 2012, [http://www.pcworld.com/article/250197/the_15_worst_data_security_breaches_of_the_21st_century.html]

Art. 8 EU Charter Fundamental Rights

Assaf D., Models of critical information infrastructure protection, International Journal of Critical Infrastructure Protection, Volume 1, Pages 6–14, December 2008, [http://ac.els-cdn.com/S1874548208000097/1-s2.0-S1874548208000097-main.pdf?_tid=1cd9c180-adcb-11e3-9c53-00000aab0f6c&acdnat=1395057542_58d0a30b9713f06f7a6a01180029def6]

Aviation Week and Space Technology, October 22, 2012, [http://www.aviationweek.com]

Aviram A. , Tor A. , Overcoming impediments to information sharing, Alabama Law Review 55 (2), pag. 231-279, 2004

Baker L., 2010 USA - Telecoms, Wireless, Broadband and Forecasts, 2010

Baker S. *et al*., In The Crossfire: Critical Infrastructure In The Age Of Cyber War 3, Mcafee, Inc., 2009, [http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf]

Baltzan P., Phillips A., Detlor B., Business-driven information systems, 1st Canadian Ed. Whitby, Ontario, Canada: McGraw-Hill Ryerson, 2008

Barlow J. P., The netizen: the powers that were, Wired, 4(9) , 53–56, 195, 197, 199, 1996

BBC, Passwords revealed by sweet deal, 2004, [http://news.bbc.co.uk/1/hi/technology/3639679.stm]

Belissent J., Getting clever about smart cities : New opportunities require new business models, Forrester research, 2010,[http://www.forrester.com/Getting+Clever+About+Smart+Cities+New+Opportunities+Require+New+Business+Models/fulltext/-/E-RES56701]

Bernard R., Understanding Cyber Insurance , Security Technology & Design, ISSN 1069-1804, Volume 18, no. 7, p. 16, 2008

Bohme R., Kataria G., Models and Measures for Correlation in Cyber-Insurance, Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK, June 2006

Bohme R., Schwartz G., Modelling Cyber-Insurance: Towards A Unifying Framework, Workshop on the Economics of Information Security (WEIS), Harvard, June 2010

Bolot J., Lelarge M., Cyber Insurance as an Incentive for Internet Security, Seventh Workshop on the Economics of Information Security, 25-28 June, 2008

Boritz J. E., IS Practitioners' Views on Core Concepts of Information Integrity, International Journal of Accounting Information Systems, Elsevier, 2011

Bowerman B., Braverman J., Taylor J., Todosow H., Von Wimmersperg U., The vision of a smart city, 2nd International Life Extension Technology Workshop, 2000

Branin J. (Ed.), Collection Management in the 1990s. Chicago, IL: American Library Association, 1990

Brenner S. W., Cybercrime, cyber terrorism and cyber warfare, Revue internationale de droit pénal, Vol. 77, no. 3, p. 453-471, 2006, [www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm]

Brenner S.W., Clarke L.L.., Civilians in Cyber warfare: Conscripts, Vanderbilt Journal of Transnational Law, Vol. 43, 1011, 2010

Brenner S.W., Cyber threats: The Emerging Fault Lines of the Nation State, pp. 71–161, 2009

Brinkman J., Supporting sustainability through smart infrastructures: the case of Amsterdam, Network Industries Quarterly , vol. 13, no 3, 2011, [http://newsletter.epfl.ch/mir/index.php?module=epflfiles&func=getFile&fid=244&inline=1]

Brinkman J., Supporting sustainability through smart infrastructures: the case of Amsterdam, NGInfra Conference, Virginia Beach, November 2011, [http://sinfras.com/conferences/nginfra2011/files/2011/12/NGInfra_2011_Amsterdam.pdf]

Brömmelhörster J., Fabry S., Wirtz N., Critical Infrastructure Protection: Survey of World-Wide Activities, 2004,[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.pdf?__blob=publicationFile]

Buckler G., Can you afford to lose your data? How to insure your company's electronic files is a growing issue, and more needs to be done to address it, The globe and Amil, 2005

Cabinet Office, Sector Resilience Plans for Critical National Infrastructure 2010, March 2010

Caldwell T., Ethical hackers: putting on the white hat, Network Security, Volume 2011, Issue 7, Pages 10–13, July 2011, [http://ac.els-cdn.com/S1353485811700757/1-s2.0-S1353485811700757-main.pdf?_tid=754aba56-d4f7-11e3-8521-00000aab0f6c&acdnat=1399364684_269af6e21b6eef1ff5476f83cfcda69c]

CAMM steering committee, CAMM response to cloud computing: a consultative document, 22nd may, 2011

Capgemini, Using insurance to mitigate cybercrime risk, Challenges and recommendations for insurers, 2012

Càrdenas A.A., Radosavac S., Grossklags J., Chuang J., Hoofnagle C., An Economic Map of Cybercrime, The 37th Research Conference on Communication, Information and Internet Policy (TPRC), George Mason University Law School, Arlington, 25th September, 2010

Cateddu D., Security - Resilience in Governmental Clouds, ENISA, 2011, [https://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds]

Caudle D.L., Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers, University of Phoenix, School of Advanced Studies, 2010

Center for Strategic and International Studies, The Economic Impact Of Cybercrime And Cyber Espionage, July 2013, [http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf]

Centre for Security Studies (CSS), Focal Report 1 Critical Infrastructure Protection, Crisis and Risk Network (CRN), 2008, [http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/publikationen_ski.parsys.71944.DownloadFile.tmp/focalreport1.pdf]

CESG, Guide to IA Self-Assessment Using the HMG IA Maturity Model and Assessment Framework, 2013

CESG,HMG IA Standard No.1 - Technical Risk Assessment , Issue 3.51, October 2009, [http://www.cesg.gov.uk/publications/media/policy/is1_risk_assessment.pdf]

CESG,HMG information assurance maturity model and assessment framework, CESG, 27th may,2010

Chaffey N., People power: making your people an essential part of your cyber security strategy, [http://www.paconsulting.com/our-thinking/why-a-human-side-is-essential-to-effective-cyber-security/]

Choo C. W., [http://choo.fis.utoronto.ca/Imfaq/], 2008

Clemente D., Cyber Security and Global Interdependence: What Is Critical?, Chatham House, Feb 2013, [http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf]

CNSSP No. 22, Policy on Information Assurance Risk Management for National Security Systems, Committee on National Security Systems, January 2012, [http://www.ncix.gov/publications/policy/docs/CNSSP_22.pdf]

Colwill C .J., Todd M. C., Fielder G. P., Natanson C., Information assurance, Technology Journal, Volume 19, no 3, pp. 107 - 114 ,07/2001, [http://download.springer.com/static/pdf/166/art%253A10.1023%252FA%253A1011998517801.pdf?auth66=1395582573_bc478b20a703fcd7e6c9cc92862a6acc&ext=.pdf]

Commission of European Parliament, COM(2007) 267- Towards a general policy on the fight against cyber crime, 2007, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF]

Commission of European Parliament, COM(2007) 267- Towards a general policy on the fight against cyber crime, 2007

Commission of the European Communities, Green paper on a European Programmes for Critical Infrastructure Protection COM(2005)576, 2005

Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, European Commission Working paper, 2013

Common Assurance Maturity Model Steering Committee, Common Assurance Maturity Model Guiding Principles, 2010,[http://common-assurance.com/resources/Common-Assurance-Maturity-Model-vision.pdf]

Communication from the Commission on a European Programme for Critical Infrastructure Protection, 12th December 2006

Conference on Information Law and Policy for the Information Economy, organized by Professors Branscomb L.M., Mayer-Schönberger V. of Harvard University's John F. Kennedy School of Government, 16th-18th June, 2005

Conrad S.H., LeClaire R.J., O'Reilly G.P., Uzunalioglu H., Critical National Infrastructure Reliability Modelling and Analysis, Bell Labs Technical Journal 11(3), 57–71, 2006, [http://www.lucent.com/enrich/v1i22007/pdf/BLTJ_20178.pdf]

Constantin L.., Most IT and security professionals see Anonymous as serious threat to their companies, Infoworld, April 23rd, 2012, [http://www.infoworld.com/d/security/most-it-and-security-professionals-see-anonymous-serious-threat-their-companies-191502]

Council Directive 2008/114/EC of 8 December 2008

Counter-terrorism strategy [www.security.homeoffice.gov.uk]

Critical infrastructure- Resilience strategy, Australian government, 2010

Cukier K., Ensuring (and Insuring?) Critical Information Infrastructure Protection, Rueschlikon Conference on Information Policy, 2005, [http://www.vmsweb.net/attachments/pdf/R-05_Report_Online.pdf]

Cybercrime Report: The Human Impact, Symantec, 2010

Damage Toll for Nimda, less than was expected, 2001, [http://www.xatrix.org/news/damage-toll-for-nimda-less-than-was-expected--773/]

Dardick G.S., Cyber Forensics Assurance, Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, November 30th 2010, [http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1076&context=adf]

Daskala B., Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology, 2010, [http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology]

Dekker M., Liveri D., Lakka M., Incident reporting for cloud computing, ENISA, 2013, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing]

Department of the Air Force, Identification and Authentication, AFMAN 33–223, HQ USAF, Washington, 1998

Deputy Assistant Secretary of Defence, Cyber, Identity, and Information Assurance Strategy, The Office of the Assistant Secretary of Defence for Networks and Information Integration / DoD Chief Information Officer, 2009, [http://iase.disa.mil/policy-guidance/dasd_ciia__strategy_aug2009.pdf]

Desouza K. C., Hensgen T., Semiotic Emergent Framework to Address the Reality of Cyber terrorism, Technological Forecasting and Social Change, Vol. 70, no. 4, pag. 385–396, 2003

Detlor B., Information Management, International Journal of Information Management, ISSN 0268-4012, Volume 30, no. 2, pp. 103 - 108, 2010, [http://www.sciencedirect.com/science/article/pii/S0268401209001510]

Difference between a computer virus and a computer worm, USCB ScienceLine.

Digital Agenda for Europe site, [http://ec.europa.eu/digital-agenda/en/internet-things]

Dipert R.R., The Ethics of Cyber warfare, Journal of Military Ethics , Volume 9, Issue 4, Special Issue- Ethics and Emerging Military Technologies, 2010, [http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404]

Dodge M., Understanding Cyberspace Cartographies: A Critical Analysis of Internet Infrastructure Mapping, PhD Thesis, 2008

Dunn Cavelty M., Critical information infrastructure: vulnerabilities, threats and responses, ICTs and International Security, 2007

Dunn Cavelty M., Systemic cyber/in/security – from risk to uncertainty management in the digital realm, Swiss Re Centre for Global Dialogue, 15 September 2011, [http://cgd.swissre.com/features/Systemic_Cyber_In_Security.html]

Dunn M. , Mauer V. , International CIIP Handbook, vol. 2, Centre for Security Studies, Swiss Federal Institute of Technology, Zurich, Switzerland, 2006, [http://e-collection.library.ethz.ch/eserv/eth:31123/eth-31123-04.pdf]

Dyer G., Intelligence Chief in US Cyber-attack Warning, Financial Times, March 13, 2013

Eckert S., Protecting Critical Infrastructure: The Role of the Private Sector, in Guns and Butter: The Political Economy of International Security", Dombrowski, P. (Eds.), 2005, [http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf]

Egan M., Geopolitical Tensions Invade Cyberspace, FOX Business, March, 11th, 2014, [http://www.foxbusiness.com/technology/2014/03/11/geopolitical-tensions-invade-cyber-space/]

ENISA, Appropriate security measures for smart grids, 2012, a

ENISA, Cloud Computing Security Risk Assessment, 2009, b, [https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment]

ENISA, Critical Cloud Computing-A CIIP perspective on cloud computing services, 2013, a, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing]

ENISA, ENISA Smart Grid Security Recommendations, 2012, d

EU Charter Fundamental Rights

EU Commission, Achievements and next steps: towards global cyber-security, 2011, a, [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0163&from=EN]

EU Commission, Protecting Europe from large scale cyber-attacks and disruptions: enhancing
preparedness, security and resilience,2009, [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&from=EN]

European Commission , Energy infrastructures: increasing security of supply in the Union, Memo, DG for Energy and Transport, 2003

European Commission, Proposal amending Council Directive 2008/114/EC Identification and designation of European critical infrastructures, Version 1, August 2011b, [http://ec.europa.eu/governance/impact/planned_ia/docs/2012_home_010_directive_critical_infrastructures_en.pdf]

European Communication 149/2009

European Communication 786/2006

Everett C., The lucrative world of cyber-espionage, Computer Fraud & Security, Volume 2009, Issue 7, Pages 5–7, July 2009, [http://ac.els-cdn.com/S1361372309700843/1-s2.0-S1361372309700843-main.pdf?_tid=2b5efe30-d4f6-11e3-972d-00000aacb362&acdnat=1399364130_1869f41c1e2791b5201503549a01ea5c]

Executive Order 13228. Section 3 (e) (i), (ii), (iv), (v) and (vi), pp. 51813-51814

Executive Order 13010. p 37347, 15th July 1996

Executive order 13636 : Improving critical infrastructure security, department of homeland security, 12th june,2013,

Finklea K. M., Theohary C.A., Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, Congressional Research Service, 9th January, 2013, [http://www.fas.org/sgp/crs/misc/R42547.pdf]

Frigo M.L., Anderson R.J., What Is Strategic Risk Management?, Strategic Finance, April 2011, [http://www.markfrigo.com/What_is_Strategic_Risk_Management_-_Strategic_Finance_-_April_2011.pdf]

Furnell S.M., Warren M.G., Computer hacking and cyber terrorism: the real threats in the new millennium?, Computers & Security, Volume 18, Issue 1, Pages 28–34, 1999, [http://ac.els-cdn.com/S0167404899800066/1-s2.0-S0167404899800066-main.pdf?_tid=df0726e6-d4f7-11e3-a01c-00000aacb35f&acdnat=1399364861_7cd8df0fa2916ed473a3f6461220f4e0]

Geers K., Kindlund D., Moran N., Rachwald R., World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, FireEye Labs, 2013, [http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf]

Geers K., The Cyber Threat to National Critical Infrastructures: Beyond Theory, Information Security Journal: A Global Perspective, Vol. 18, Issue 1, p1-7. 7p, 2009, [http://se5fj2qs2v.scholar.serialssolutions.com/?sid=google&auinit=K&aulast=Geers&atitle=The+cyber+threat+to+national+critical+infrastructures:+Beyond+theory&id=doi:10.1080/19393550802676097&title=Information+security+journal.&volume=18&issue=1&date=2009&spage=1&issn=1939-3555]

Gengler B., Politicians Speak Out on Cyber terrorism, Network Security, 10,pag. 6, 1999

German Federal Ministry of the interior , Protecting Critical Infrastructures – Risk and Crisis Management

Gheorghe A.V., Masera M., de Vries L., Weijnen M., Kroger W., Critical infrastructures: the need for international risk governance, International Journal of Critical Infrastructures, Vol.3, No.1/2, pp.3 - 19, 2007, [http://www.nextgenerationinfrastructures.eu/download.php?field=document&itemID=449529]

Givens A. D. , Busch N. E. ,Realizing the promise of public-private partnerships in U.S. critical infrastructure protection, International Journal of Critical Infrastructure Protection, Volume 6, Issue 1, Pages 39–50, March 2013, [http://ac.els-cdn.com/S187454821300005X/1-s2.0-S187454821300005X-main.pdf?_tid=3e1cafe8-adca-11e3-a503-00000aab0f26&acdnat=1395057168_301d295d8707db05293ee5c6011119b0]

Gonzàlez Fuster G., Gutwirth S., The core content of personal data protection: a conceptual controversy, PRESCIENT International Conference, 28th Nov.2012, [http://www.prescient-project.eu/prescient/inhalte/download/4-Gonzales-Fuster.pdf]

Gorniak S., *et al*., Priorities for Research on Current and Emerging Network Technologies, ENISA, 2010, [https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/procent]

Government Accountability Office, Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats- GAO-07-705, 2007, [http://www.gao.gov/new.items/d07705.pdf]

Graham A., Canada's critical infrastructure -When is Safe Enough Safe Enough?, National security strategy for Canada series, The Macdonald-Laurier Institute, 2011, [http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf]

Grauman B., Cyber-security: The vexed question of global rules - An independent report on cyber-preparedness around the world, Security & Defence Agenda, 2012, [http://www.mcafee.com/au/resources/reports/rp-sda-cyber-security.pdf]

Green Paper - A European Strategy for Sustainable, Competitive and Secure Energy, COM/2006/0105 final

Hahn R. W., Layne-Farrar A., The Law and Economics of Software Security, Harvard Journal of Law and Public Policy, 30(1): 283-353, 2006

Hallinan D., Friedewald M., McCarthy P., Citizens' Perceptions of Data Protection and Privacy in Europe, Computer law and security review, Vol. 28, No 3, pp. 263-272, 2012

Hamill J.T., Deckro R.F., Kloeber J.M., Evaluating information assurance strategies , Decision Support Systems, Volume 39, Issue 3, Pages 463–484, May 2005, [http://ac.els-cdn.com/S0167923604000284/1-s2.0-S0167923604000284-main.pdf?_tid=e0ac61dc-b107-11e3-92ad-00000aacb361&acdnat=1395413494_cb1b040578a40c17b4e294d3cfd89e51]

Hammerli B., Renda A., Protecting critical infrastructure in the EU, CEPS task force report, 2010

Hardin G., The tragedy of the commons, Science 13 (162), pag. 1243–1248, 1968

Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan H., Perdue W., Spiegel J., The Law Of Cyber-Attack, California Law Review, Vol. 100, No. 4, August 2012, [http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf]

Healey J., Grindal K., A Fierce Domain: Conflict in Cyberspace, 1986-2012 , Cyber Conflict Studies Association, 2013

Herath H.S.B., Herath T.C., Copula-based actuarial model for pricing cyber-insurance policies, 2011

Herath H.S.B., Herath T.C., Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management, 2006

Hesseldahl A., Cisco Reminds Us Once Again How Big the Internet Is, and How Big It's Getting, All Things D, 14 July 2011, [https://allthingsd.com/20110714/cisco-reminds-us-once-again-how-big-the-internet-is-and-how-big-its-getting/]

Hildreth S.A., Cyber warfare, Congressional Research Service, June 19, 2001, [http://www.fas.org/irp/crs/RL30735.pdf]

Hinde S., Cyber Wars and other threats, Computers & Security, Volume 17, Issue 2, Pages 115–118, 1998

Hinde S., Cyber-terrorism in context, Computers & Security, Volume 22, Issue 3, Pages 188–192, April 2003, [http://ac.els-cdn.com/S0167404803003031/1-s2.0-S0167404803003031-main.pdf?_tid=ad8b2362-d4f5-11e3-93c7-00000aab0f27&acdnat=1399363919_66a5531b754095c9ffe538c94015d570]

Hinde S., Incalculable potential for damage by cyber-terrorism, Computers & Security, Volume 20, Issue 7, Pages 568–572, 31 October 2001, [http://ac.els-cdn.com/S0167404801007040/1-s2.0-S0167404801007040-main.pdf?_tid=9793463c-d4f7-11e3-b3c3-00000aacb360&acdnat=1399364741_97074ecb4c451fee70b11b5f64f5c0eb]

Holt M.W., Critical Infrastructure Protection in the European Union, The CIP report, May 2013

Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, 2013, [http://mutualink.net/PDF/NIPP-2013-Partnering-for-Critical-Infrastructure-Security-and-Resilience-Dec-2013.pdf]

Hromada M., Lukas L., Critical Infrastructure Protection and the Evaluation Process, International Journal of Disaster Recovery and Business Continuity, Vol.3, 2012,[http://www.sersc.org/journals/IJDRBC/vol3/5.pdf]

Hua J., Bapna S., The Economic Impact of Cyber Terrorism, The Journal of Strategic Information System, Vol. 22, no.2, pag. 175-186, June 1, 2013

Huffaker B., Fomenkov M., Claffy kc, Internet Topology Data Comparison, Cooperative Association for Internet Data Analysis (CAIDA), May 2012, [http://www.caida.org/publications/papers/2012/topocompare-tr/topocompare-tr.pdf]

Huntley T.C., Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change, Nature of Warfare, 2010

I Love You, WHoWhatWhereWhenWhy.com

IAAC Dependencies and Risk Working Group, Policy paper, July 2000

IACC, IAAC's Identity Assurance Programme 2006-2008: Concluding Report, September 2008, [http://www.iaac.org.uk/_media/IdAConcludingReportSept08.pdf]

ICE, The state of the nation : Defending critical infrastructure, 2009

Industry security notice, 2010

Information & Records Management Officer, Information Management Strategy, Cumbria Constabulary, 2009

Information Management Strategy, Alberta service, 2013, [http://www.im.gov.ab.ca/documents/publications/Information_Management_Strategy_FINAL.pdf]

Information Management Strategy, In-Form email Management, 2004, [http://dlmforum.typepad.com/Information_Management_Strategyv1.pdf]

Internet World Stats, 2012, [http://www.internetworldstats.com/stats.htm]

ITU-T Recommandation Y.2001, [http://www.itu.int/rec/T-RECY.2001-200412-I/en]

Jamasb T., Pollitt M., Electricity Market Reform in the European Union: Review of Progress toward Liberalization & Integration, Centre for Energy and Environmental Policy Research, 2005, [http://18.7.29.232/bitstream/handle/1721.1/45033/2005-003.pdf?sequence=1]

Janczewski L. J., Colarik A M., eds., Cyber Warfare and Cyber Terrorism, Hershey (PA), Information Science Reference, 2008

Juster K. I., Tritak J.S., Critical Infrastructure Assurance: A Conceptual Overview, in: Joint Economic Committee, United States Congress: Security in the Information Age – New Challenges, New Strategies (Washington, DC: White House), p. 12, 2002

Kameda T., Tsukasaki T., Hastie R., Berg N., Democracy uncertainty: The wisdom of crowds and the free-rider problem in group decision making, Psychological Review Vol, 118, Issue 1, pag. 76–96, 2011

Kapto A.S., Cyber warfare: Genesis and doctrinal outlines, Herald of the Russian Academy of Sciences, Volume 83, Issue 4, pp 357-364, July 2013, [http://download.springer.com/static/pdf/458/art%253A10.1134%252FS1019331613040023.pdf?auth66=1399802684_901c984d3238ffbc752deaa2d6473827&ext=.pdf]

Katz D.M. , Companies Counterattack Cyber Villains, 20th August, 2013, a, [http://ww2.cfo.com/risk-management/2013/08/companies-counterattack-cyber-villains/]

Katz D.M., Data Threats Spark Insurance Hunger, 21st August, 2013 , b, [http://ww2.cfo.com/risk-management/2013/08/data-threats-spark-insurance-hunger/]

Kim W., Jeong O., Kim C., So J., The dark side of the Internet: Attacks, costs and responses, Information Systems, Volume 36, Issue 3, Pages 675–705, Special Issue on WISE 2009 - Web Information Systems Engineering, May 2011,[http://ac.els-cdn.com/S0306437910001328/1-s2.0-S0306437910001328-main.pdf?_tid=29659b26-d4f5-11e3-bcd8-00000aacb360&acdnat=1399363697_406bac77fa7965db757e74c9658fc2fa]

Kramer A.,E-mail spam falls after Russian crack down, The New York Times, October 26,2010

Kramer F.D., Teplinsky M.J., Cybersecurity and Tailored Deterrence, Atlentic Council, 2014, [http://www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf]

Kshetri N., Pattern of global cyber war and crime: A conceptual framework, Journal of International Management, Volume 11, Issue 4 Pages 541–562, Global Security Risks and International Competitiveness, December 2005, [http://ac.els-cdn.com/S1075425305000700/1-s2.0-S1075425305000700-main.pdf?_tid=d58c29fa-d4f6-11e3-8952-00000aacb35e&acdnat=1399364416_35fefc7f45fe0cfab6c4c860a2aed617]

Lancaster H., Europe - Telecommunications Infrastructure and NGNs, 2013

Landry C. E., Li J., Participation in the Community Rating System of NFIP: Empirical Analysis of North Carolina Counties, Natural Hazards Review, 13(3): 205–220, 2012

Larson R., Marks D., Dahleh M., Ilic M., The 3 R's of Critical Energy Networks: Reliability, Robustness and Resiliency, MIT Energy Research Council, 2005, [http://cesf.mit.edu/papers/ThreeRs.pdf]

Lelarge M., Bolot J., Economic incentives to increase security in the internet: The case for insurance, Proceedings - IEEE INFOCOM, ISSN 0743-166X, ISBN 9781424435135, pp. 1494 - 1502, 2009

Levy, M., Salvadori, M., Why Buildings Fall Down, *W.W*. Norton & Compan, New York, 1992

Lewis A. M. , Ward D., Cyra L. , Kourti N., European Reference Network for Critical Infrastructure Protection, International Journal of Critical Infrastructure Protection, Volume 6, Issue 1, Pages 51–60, March 2013, [http://ac.els-cdn.com/S1874548213000073/1-s2.0-S1874548213000073-main.pdf?_tid=411f4b2e-adca-11e3-a116-00000aab0f6b&acdnat=1395057174_b02a376d678d7f7466871309a9791c50]

Lewis J. A., Assessing the risks of cyber terrorism, cyber war, and other cyber threats, 2002, [http://www.dtic.mil/dtic/]

Lewis T.G., Critical Infrastructure, Protection in homeland security-Defending a Networked Nation, Wiley Interscience, 2006, [http://books.google.it/books?hl=en&lr=&id=xoICniGegE0C&oi=fnd&pg=PR5&dq=critical+infrastructure+structure&ots=sC4M51MiY5&sig=8VWC5wdriXgukujcBg-8ZCuuqrc#v=onepage&q=critical%20infrastructure%20structure&f=false]

Little R.G., Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems, 36th Hawaii International Conference on System Sciences, 2002, [http://www.computer.org/csdl/proceedings/hicss/2003/1874/02/187420058a.pdf]

Lord Jopling (Special Rapporteur), 162 CDS 07 E rev 1 – The Protection of Critical Infrastructures, 2007

Markoff J., A Code for Chaos, New York Times, October 2, 2010, [http://www.nytimes.com/2010/10/03/weekinreview/03markoff.html]

Marsh, Benchmarking Trends: More Companies Purchasing Cyber Insurance, March 2013, [http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch/ID/29870/Benchmarking-Trends-More-Companies-Purchasing-Cyber-Insurance.aspx]

Marsh, Cyber Risk: Trends And Solutions, 2013, [http://usa.marsh.com/Portals/9/Documents/Marsh%20NROR%20September%202013%20Cyber%20Risk.pdf]

Màtl O., Smarter Cities as an European Agenda , IBM, 2010, [http://www-05.ibm.com/cz/public/pdf/Chytrejsi_mesta_jako_evropske_tema.pdf]

McAfee Labs, Global Energy Cyberattacks - “Night Dragon”, 2011

McAfee, Operation "Aurora" Hit Google, Others, 2010

Morningstar C., Farmer F.R., The Lessons of Lucas film's Habitat. The New Media Reader, Ed. Wardrip-Fruin and Nick Montfort: The MIT Press, 2003. 664-667

Moteff J., Parfomak P., Critical Infrastructure and Key Assets: Definition and Identification, CRS Report for Congress, 2004, [http://www.dtic.mil/dtic/tr/fulltext/u2/a454016.pdf]

Moteff J., Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, The Library of Congress, 2005, [http://www.fas.org/sgp/crs/homesec/RL32561.pdf]

Moteff J.D., Critical Infrastructures: Background, Policy and implementation, Report for Congress, 2002

Murer R., Internet of Things – Fundamentals, Agencia Click Isobar, 2010, [http://www.theinternetofthings.eu/content/internet-things-%E2%80%93-fundamentals-ricardo-murer]

Näf M., Ubiquitous Insecurity? How to 'Hack' IT Systems, Information & Security: An International Journal, no. 7, pp. 104–118, 2001

National Critical Information Infrastructure Protection Centre (NCIIPC), 2013

National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009, 2006

National Research Council, Making the Nation safer: The role of Science and Technology in Countering Terrorism, Committee on Science and Technology for Countering Terrorism, National Academy of Sciences, 2002 , [http://www.aaas.org/sites/default/files/migrate/uploads/ch23.pdf]

National Strategy for Critical Infrastructure Protection, CIP Strategy, Federal Republic of Germany
Federal Ministry of the Interior, 2009,
[http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf]

National Strategy for Critical Infrastructure Protection, CIP Strategy, 2009

NATO Cooperative Cyber Defense Centre of excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013, [http://web.archive.org/web/20140306081257/http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf]

NISRA, Information Assurance policy statement by UK census office, June 2011

NIST, Improving Critical Infrastructure Cyber security Executive Order 13636 - Preliminary Cyber security Framework, 2014, [http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf]

Norton Cybercrime Report, 2011

OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, 2002, [http://www.oecd.org/sti/ieconomy/15582260.pdf]

OECD Ministerial background report, Development of policies for protection of critical information infrastructures, 17th-18th June, 2008, [http://www.oecd.org/sti/40761118.pdf]

OECD recommendation of the council on the protection of critical information infrastructures, OECD ministerial meeting on the future of the Internet economy, 17th-18th June, 2008, [http://www.oecd.org/sti/40825404.pdf]

OECD, Shaping policies for the future of the Internet Economy, OECD Ministerial Meeting on the Future of the Internet Economy, 2008, [http://www.oecd.org/internet/ieconomy/40821707.pdf]

Ogut H., Menon N., Raghunatan S., Cyber Insurance and IT Security Investment : Impact of Interdependent Risk, University of Texas, 2004

Orszag P., Homeland and the Private Sector: Testimony before the National Commission on Terrorist Attacks Upon the United States, 19 November 2003, [http://www.brookings.edu/views/testimony/orszag/20031119.pdf]

Paget F., Hacktivism- Cyberspace has become the new medium for political voices, McAfee white paper, 2012

Pal R., Golubchik L., Psounis K., Aegis-A Novel Cyber-Insurance Model, University of Southern California, 2011

Pal R., Hui P., Cyber Insurance for Cyber Security- A Topological Take On Modulating Insurance Premiums, SIGMETRICS Performance Evaluation Review 40(3): 86-88, 2012

Pal R., Hui P., Cyber Insurance for Cyber Security- A Topological Take On Modulating Insurance Premiums, SIGMETRICS Performance Evaluation Review 40(3): 86-88, 2012

Passive Infrastructure Sharing in Telecommunications, kpmg, 2011, [http://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Passive-Infrastructure-Sharing-in-Telecommunications.pdf]

Pederson P. , Dudenhoeffer D. , Hartley S., Permann M. , Critical Infrastructure Interdependency Modelling: A Survey of U.S. and International

Research, Idaho National Laboratory, August 2006, [http://cipbook.infracritical.com/book3/chapter2/ch2ref2a.pdf]

Perks J., Hyde J., Falconer A., Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector, Final Report to European Commission Directorate-General Justice, Freedom and Security, 4th September, 2009, [http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf]

Perrin C., The CIA Triad, 2008,[http://www.techrepublic.com/blog/it-security/the-cia-triad/#]

Pfanner E., Europe unleashes online gambling to fill coffers, The New York Times, July 27,2010

Ponemon Institute LLC, Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, august 2013

Power System Outage Task Force — Final Report on the 14 August 2003 Blackout in the United States and Canada: Causes and Recommendations," 2004

President Releases National Strategy for Homeland Security, 16 July, 2002, [http://www.hsdl.org/?view&did=474932]

President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations: Thinking Differently, GPO, Washington, 1997

President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, The White House, Washington, DC , 1997 [chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf]

Presidential Policy Directive 21 (PPD-21)-Critical Infrastructure Security and Resilience, 2013

Renn O., Risk Governance Towards an integrative approach, International Risk Governance Council, 2005, [http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf]

Reponen T., Information management strategy — an evolutionary process, Scandinavian Journal of Management, Volume 9, Issue 3, Pages 189–209, September 1993, [http://ac.els-cdn.com/095652219390016L/1-s2.0-095652219390016L-main.pdf?_tid=8d1badf4-cef1-11e3-8a61-00000aab0f27&acdnat=1398702440_731dd8aa4ff238688e917925eb044a6f]

Report on Critical Infrastructure protection; Ministry of the Interior 16/9/05

Riptech, Riptech Internet Security Threat Report, vol II, July 2002 , [http://www.4law.co.il/276.pdf]

Ritholtz B., Timeline of Cyber-Attacks from China, 2013, [http://www.ritholtz.com/blog/2013/02/china-cyber-attacks/]

Roberts A., Wallace W., McClure N., Strategic Risk Management, Edinburgh Business School, 2012, [http://www.ebsglobal.net/documents/course-tasters/english/pdf/h17rk-bk-taster.pdf]

Roper C. , Risk Management for Security Professionals, Butterworth-Heinemann, 1999

Rosen P.K. *et al.*, Cyber Insurance: A Last Line of Defense When Technology Fails, Latham & Watkins, April 15th, 2014

Rowlands D., Devlin A., Critical Energy Infrastructure Protection Policy Research Series-Insurance and Critical Infrastructure Protection Is there a Connection in an Environment of Terrorism? , n°8, 2006

Samani R., Common Assurance Maturity Model (CAMM)- The new business assurance barometer, CTO Cyber Security Forum, 2010, [http://www.fstech.co.uk/fst/FSTech_Conference_2011/Common_Assurance_Maturity_Model_Raj_Samani.pdf]

Sarrocco C., Ypsilanti D., Convergence and Next-Generation Networks , OECD, 2008, [http://www.oecd.org/sti/40761101.pdf]

Schelling T., Arms and Influence, New Haven: Yale University Press, 1966

Schmidt E., Cohen J., The New Digital Age: Reshaping the Future of People, Nations and Business, Knopf, 2013

Schultz E. E., A framework for understanding and predicting insider attacks, Proc. Of Compsec, pages 526–531, London, UK, October 2002

Sherstobitoff R., Analyzing Project Blitzkrieg, a Credible Threat, McAfee white paper, 2012

Shetty N., Schwartz G., Felegyhazi M., Walrand J., Competitive Cyber-Insurance and Internet Security, Economics of Information Security and Privacy, 229-247, 2010

Soafer A. D., The Best Defense? Legitimacy and Preventive Force, Stanford, Hoover Institution Press, 2010

Stanton, J.J., Terror in Cyberspace, American Behavioral Scientist, Vol. 45, no.6, pag.1017–1032, 2002

Strategic risk management, NYU Stern School of Business, [http://people.stern.nyu.edu/adamodar/pdfiles/papers/strategicrisk.pdf]

Suter M., A Generic National Framework For Critical Information Infrastructure Protection (CIIP), International telecommunication unit, 2007, [http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf]

Tatum M., What Is a Cyber-attack?, 2010, [http://www.wisegeek.com/what-is-a-cyberattack.htm]

Thales, A practical guide to assessing your cyber security strategy, White paper, March 2012

The American Heritage Dictionary of the English Language, Fourth Edition, Houghton,2000

The Department of Commerce- Internet Policy Task Force, Cyber security, Innovation and the Internet Economy, June 2011, [http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf]

The Parliamentary Office of Science and Technology, Resilience of UK Infrastructure, no 362, 2010, [http://www.google.it/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=6&cad=rja&ved=0CF8QFjAF&url=http%3A%2F%2Fwww.parliament.uk%2Fbriefing-papers%2Fpost-pn-362.pdf&ei=uVcHU_fWI4el4ASk_YHwCw&usg=AFQjCNEZWRq81ObgzipvBaIr3uUB1iZhUQ&sig2=7kPJjrJYNF0_vW7Tl0zTzA&bvm=bv.61725948,d.bGQ]

The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought, Business Insider,20 November 2013, [http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11]

Thissen W.A.H., Herder P.M. (Eds.), Critical Infrastructures. State of the Art in Research and Application, Kluwer Academic, 2003

Townsend A. M., Moss M.L., Telecommunications infrastructure in disasters: Preparing cities for crisis communications, Centre for Catastrophe Preparedness and Response and Robert F. Wagner Graduate School of Public Service New York University, 2005, [http://www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf]

Trimintzios P., Hall C., Clayton R., Anderson R., Ouzounis E., Resilience of the Internet Interconnection Ecosystem, ENISA, 2011, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report]

U.S. Intelligence Community's March 2013 Worldwide Threat Assessment, [www.intelligence.senate.gov/130312/clapper.pdf]

U.S. Office of Homeland Security. July 16, 2002

UK Government Actuary's Department, A practical guide to strategic risk management, 28th August, 2013, [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/256431/A_Practical_Guide_to_Strategic_Risk_Management.pdf]

Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001, PUBLIC LAW 107–56—OCT. 26, 2001, [http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf]

US Department of Defence Directive 8500.1, Information Assurance, October 24, 2002

US Department of Homeland Security, Blueprint for a Secure Cyber Future: The Cyber security Strategy for the Homeland Security Enterprise, November 2012, [http://www.dhs.gov/files/publications/blueprint-for-a-secure-cyber-future.shtm]

US Government, H. R. 2281 Digital Millennium Copyright Act , 1998

US Government's Paperwork Reduction Act of 1980

US Homeland Security, Cyber security Insurance workshop, 2012, [http://www.dhs.gov/publication/cybersecurity-insurance]

van Eeten M.J.G. , Roe E.M., Schulman P., de Bruijne M.L.C. , The Enemy Within: System Complexity and Organizational Surprises, in M. Dunn and V. Mayer (eds), International CIIP Handbook 2006. Vol. II: Analyzing Issues, Challenges, and Prospects, Zurich, Center for Security Studies at ETH Zurich, pp. 89–109, 2006, [www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157>]

Vanston L.K., Hodges R.L., Forecasts for the US Telecommunications Network, Telenor ASA, 2009, [http://www.tfi.com/pubs/w/pdf/telektronikk_telecom.pdf]

Virilio P., Lotringer S., Pure War, New York: Semiotext, 1983

WBGU , World in Transition – Strategies for Managing Global Environmental Risks, Annual Report, 1998

Wehde E.,US Vulnerable to Cyber terrorism, Computer Fraud & Security, pag. 6-7, 1998

Wenger A., Metzger J., Dunn M., International CIIP Handbook- An inventory of protection policies in eight countries, Centre for Security Studies, ETH Zurich, 2002, [http://e-collection.library.ethz.ch/eserv/eth:31123/eth-31123-01.pdf]

What is critical infrastructure?, Australian National Security, [www.ag.gov.au/agd]

Wilke B.J., A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events, Carnegie Mellon University, 2007

Wilsker I., Cyber Crime, Cyber Terrorism, Cyber War, [http://apcug2.org/sites/default/files/cybercrime_cyberterrorism_cyberwar_apcug80412.pdf]

Wilson C., Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. CRS Report for Congress, January 29th, 2008

Wired, Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise, 2007, [http://www.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=1]

World Wide Web Size, 2014, [http://www.worldwidewebsize.com/]

Zacaria F., Big Data, Meet Big Brother. If computers can now predict our behaviour, should governments watch our every movie?, in Time 8-15 July, 2013