LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of Business and Management

Chair of Risk Management

OUTBREAK AND TREATMENT OF TERRORISM RISK. EMPIRICAL EVIDENCES FROM THE U.S. AIRLINE INDUSTRY AFTER SEPTEMBER 11TH.

Supervisor
Professor Gianluca Mattarocci

Co-supervisor
Professor Mario Comana

Candidate
Filippo Moriconi

Student ID
684811

Academic year
2017/2018

TABLE OF CONTENTS

Introduction

The entire work is focused on providing an extended analysis on terrorism risk and the evolution of the risk management techniques applied by U.S. airline companies after the terroristic attacks of September 11th, 2001.

The terroristic actions of 9/11, were a turning point in the worldwide history, being the greatest terroristic attack ever happened, which has caused 2996 casualties and more than 32 billion dollars of property damages, and moreover, it has dramatically worsened the OECD countries and Muslim states relationships, since from that day the "War on Terror" has begun (Kibble, 2002 and Blomberg, Hess, 2009). At the same time, the inadequacy of the anti-terrorism measures implemented by the U.S. aviation sector was highlighted, demonstrating the clear need for a renewal process in order to improve the inefficient security measures that have allowed to 19 terrorists to hijack four different aircrafts.

Therefore, the first goal of the work is introducing and analyzing the numerous changes that have affected the insurance industry and the risk management sector after September 11th. These changes are illustrated in terms of new security measures, new terrorism risk models in order to enhance the capability of preventing and mitigating other terrorist attacks, new insurance and reinsurance policies developed to safeguard the private insurance market and finally, innovative risk financing alternatives to hedge against terrorism risk (Webel, 2013 and Bruggeman, 2007). The study also wants to underline the crucial role played by Governments, more specifically, the key role played by the U.S. Central Authority, in this difficult situation. They were able to restore citizens well-being and economic development by promoting a fruitful collaboration between national institutions and private companies, which was the base for accelerating the economic and social recovery, and obtaining the most effective results (Aradau, Van Munster, 2007 and Michel-Kerjan, 2012).

The second main point of the work is the analysis of the specific effects of the terrorist attacks of September 11th on the U.S. airline industry, by providing tables and charts in which are resumed the principle effects of the event and, the principal changes in security policies applied by U.S. aviation enterprises (Belobaba, Hernandez, Jenkins, Powell, Swelbar, 2011). The work underlines the strong response made by the U.S. Government in order to mitigate the 9/11 negative consequences, by applying innovative and more effective security measures and insurance and reinsurance programs and, by creating more suitable risk management frameworks for preventing terrorism activities, especially against a crucial sector such as the airline industry ((Elias, Tang, Webel, 2014 and Cha, Ellingwood,

Shafieezadeh, 2015). The study is also focused on providing a cost-benefit analysis of the new airline procedures in order to define which are the most cost-effective in hedging against terrorism risk.

At the end, the work highlights the relevance of risk management techniques in improving companies' value, thanks to their capacity to predict and mitigate incoming threats and risk and therefore, to provide both more reliable economic and financial figures and lower uncertainty level for stakeholders (Mazzarella, 2005 and Yilmaz, 2008).

The study comprehends three chapters divided in sections and subsections.

The first chapter provides the definition and consequently the analysis of terrorism risk. Thereby, it is focused on underling the origins of terrorism risk and the numerous difficulties encountered in developing the correct risk management instruments for hedging this very unpredictable risk (OECD, 2005).

Chapter one is therefore divided in three main sections. The first one, principally illustrates the changes that have involved the Enterprise Risk Management and the treatment of the operational risks. This last type of risks is introduced and analyzed because terrorism risk is part of disaster risks (man-made disasters), which is, in turn, a subcategory of operational risks (Segal, 2011). Consequently, the section gives the definition of disaster risks and provides its main characteristics by introducing the Disaster Risk Framework (Baas, Ramasamy, Dey de Pryck, and Battista, 2008). Section two instead makes an historical digression about terrorism, investigating the several difficulties encountered in giving a univocal definition of this phenomenon and in outlining its different forms (Roser, Nadgy and Ritchie, 2016). Hence, this section provides a deep examination of terrorists' goals and strategies and furthermore, a table that illustrates the worst terroristic attacks in the worldwide history. In the last section of chapter one, is explained the concept of terrorism risk and its relationship with the modern risk society (according to Beck works). Moreover, section three describes the main characteristics of terrorism risk and the large number of difficulties encountered in the successful implementation of risk management measurement for hedging against it (Bouriaux and Scott, 2004).

The second chapter is based on providing a deep examination of conventional and unconventional methods used in the practice of hedging against terrorism risk, and furthermore, it clarifies the relevance of modelling this volatile risk in order to obtain more reliable data for preventing terrorism activities (Vickers, 2015 and Willis, Al-Shahery, 2014).

To provide deep explanations, chapter two is divided in four different sections. The first section gives an examination of the most important terroristic insurance and reinsurance policies applied by the OECD countries in response to the terrorism threat (Michel-Kerjan, 2012). More specifically, the work is focused on analyzing the numerous characteristics of the Terrorism Risk Insurance Act (TRIA), which is the reinsurance program developed by the U.S.A. to provide a strong response after the tragic events of September 11th, 2001. This act was adopted to furnish a provisional federal program base on a private-public partnership for compensating the insured losses linked to terrorism activities, for stabilizing the insurance market and preserving the insurance state regulation, and in conclusion, for protecting customers by providing available insurance policies against terrorism risk, (Kunreuther, Michel-Kerjan, 2017 and Webel, 2013). Moreover, in this section is also described the importance of the role of Governments, which provides assistance to private insurance markets in period of crisis. Instead, section two outlines the main alternative methods created by capital markets with the aim of providing an effective coverage against terrorism risk (OECD, 2005). These unconventional solutions, alternative risk financing instruments and alternative risk transfer tools, are implemented to overcome the limits of the conventional insurance and reinsurance measures. In conclusion, the section describes the two most famous alternative tools, terrorism bonds and captive insurance, applied by capital markets for providing coverage against terrorism risk (Bruggeman, 2007). The third section briefly illustrates the added value given by the activity of terrorism risk modelling, which provides a reliable and continuous flow of data very useful in preventing and mitigating the impacts of terrorist activities (Willis, Al-Shahery, 2014). Consequently, the study is focused on analyzing three different models, the Attacker-Defender model, the three variables terroristic model and the Social Network Analysis model. They all have different characteristics and limits, and they examine terrorism risk from a different perspective (Major, 2002). To conclude, the last section of chapter two explains and lists the principal benefits linked to the application of risk management measures for covering terrorism risk, demonstrating that the coverage policies provides a large number of advantages that far outweigh their implementation costs (Gold, 2004).

The last chapter gives a deep examination of the principal effects and changes happened in the U.S. airline industry due to the terrorist attacks of September 11th. The study is especially concerned to explains the innovative risk management practices and policies applied by the aviation sector in response to the huge negative consequences that the entire industry has

experiences in that years, by being directly hit by terrorists' activities (Jorion, 2012 and Rose, Blomberg, 2010).

Consequently, chapter three is divided into four sections. Section one analysis the historical background and the principal reasons that have led to the terrorist attacks of 9/11. Therefore, the work highlights the earlier conflict between OECD Catholics countries and Muslim states, by providing a better comprehensible context which can explain the clash of religions, (as it is defined by Huntington in his book) that has culminated with the tragic event of September 11th (Kibble, 2002 and Rose, Blomberg, 2010). Section two instead, uses tables and charts to elucidate firstly, the background situation of the U.S. airline industry in the 90s, by providing data about the most relevant events that have created economic difficulties for the American aviation sector, and secondly, the impact of the terrorist attacks of 9/11 on U.S. air carriers by examining the total airline demand and the market price changes in the airlines' stocks (Galeotti, 2006 and Drakos, 2004). The third section illustrates the major anti-terrorism measures developed in the U.S. aviation industry for avoiding other tragedies such as the previous one. Therefore, the work introduces the Aviation War Risk Insurance program, appositely developed after September 11th incident, the innovative Airline Security Risk Analysis framework, which provides more effective risk prevention and mitigation tools, and finally, the new pre-boarding and in flight security measures, which are divided in "22 layers of security", fifteen enforced in the airports, and the other seven applied during aircrafts flights (Elias, Tang, Webel, 2014 and Cha, Ellingwood, Shafieezadeh, 2015). The final section provides the cost-benefit analysis of the 22 layers of security to give a deep explanation of their real utility and effectiveness in preventing terrorism risk and increasing the American airline business value, and more information about their implementation costs. Furthermore, the cost-effectiveness analysis has the secondary goal of outlining the most suitable anti-terrorism measures for maximizing both security and safety for aviation passengers and airlines' economic performances, and simultaneously minimizing their costs (Stewart, Mueller, 2013 and Carter, Rogers, Simkins, 2006).

CHAPTER 1. Definition and Analysis of Terrorism Risk

1.1 Introduction

Chapter one presents the analysis and definition of terrorism risk. The goal of the chapter is to underline the origins of this new emerging threat and the several difficulties encountered in creating hedging instruments against terrorism risk (OECD, 2005), but also the importance of finding suitable coverage policies in order to avoid catastrophes such as September 11th (Amoore, De Goede, 2005 and Woo, 2002), a turning point in the world history in the war on terror.

The chapter is divided in three main sections that accurately explain three different concepts. Section one firstly explains the main changes in the Enterprise Risk Management and treatment of operational risks, by giving an accurate description of all the types of risks that compose this broad category (Segal, 2011). Secondly, the definition of disaster risk is introduced, by analyzing all its characteristics and by introducing the Disaster Risk Framework (Baas, Ramasamy, Dey de Pryck, and Battista, 2008). Disaster risks are part of the general category of operational risks, and terrorism risk is part of this smaller category. Section two is focused on describing the history of terrorism, analyzing the importance and difficulties in giving a univocal definition of this phenomenon (Roser, Nadgy and Ritchie, 2016), and explaining the different forms of terrorism (Mahmood, 2002). Goals and strategies of the principal terroristic groups are accurately described, and, at the end of the section, the worst terroristic attacks in the world history in terms of property damages are illustrated by table three (Kydd and Walter, 2006). Finally, section three introduced the concept of terrorism risk, strictly related to the modern society, otherwise called risk society (Beck, 2002). After the illustration of the risk society, by describing its features and by giving a precise definition of security and precautionary risk, a secondary investigation is made in order to understand the complex relationship between modern society and terrorism risk (Aradau and Van Munster, 2007). At the end of the section, the main characteristics of terrorism risk are explained and moreover, the wide range of difficulties is described in the application of the right measures to prevent this dangerous threat (Bouriaux and Scott, 2004).

1.2 Operational risks and Disaster risks

The section shows the changes of the new Enterprise Risk Management approach especially concerning the lately introduced operational risk. It is divided in two sub-sections: the first one gives the definition of the pre-mentioned operational risks, analyzing the main aspects and risks that compose the broad category, and the approaches used to calculate operational risks. Sub-section two defines the general category of disaster risk (that also includes terrorism risk analyzed in the following sections) by giving a careful description of all the principal factors connected with the previously mentioned category of risk. In addition, the Disaster Risk Management Framework is explained for having a better comprehension of the disaster risk's analysis.

1.2.1 The evolution of Risk Management: focus on Operational Risks.

In the latest years, the need for a more effective risk management model and a more rigorous analysis of operational risks have gained attention to regulators, therefore, it was created and successively implemented a new Basel regulatory framework[1] in order to solve these emerging issues (Chaudhuri and Ghosh, 2016). One of the main objective of the Basel Committee was to develop a new methodology focused on enhancing the operational risk assessment by encouraging industries to strengthen methods for collecting data, measuring, monitoring and mitigating all types of operational risks (Chaudhuri and Ghosh, 2016).

Risk management as corporate function is relatively recent, and its concept drastically changed from the 1980s when the process of evolution and adaptation to a new and dynamic environment started (Dionne, 2013). The several contributions in terms of classification of risks and instruments for improving their control and analysis implemented by Basel II, together with the events of the terroristic attack of September 11th, Hurricane Katrina and the global financial crisis of 2007/2008[2], underlined the clear need for a high-quality framework for the creation of a new and more effective Risk Management model in order to avoid other catastrophes (Chaudhuri and Ghosh, 2016). It became a priority for the

[1] Basel II is the new framework and it was release in 2009 and it was based on three main pillars: Minimum Capital Requirements, Supervisory Review and Market Discipline (Chavez, 2007).

[2] Other important events that have led to the improvement of Risk Management models are related to waves of accounting scandals in the early 2000s, continuous technological advancements and rare events such as H1N1 flu pandemic (Segal, 2011).

regulators to change the old silo-based risk management technique because of all its limitation in determining the overall risk appetite[3] of the firm, managing its risk exposure[4] and in providing the correct risk disclosures for all stakeholders interested. In addition, the traditional silo-based risk management was unable to:

- prioritize and manage individual key risks, there was no Individual Analysis;
- understand the integrated impact of multiple risks;
- calculate the aggregate risk exposure metrics at the enterprise level (Segal, 2011).

The implementation of the new Enterprise Risk Management (ERM) is viewed as the natural evolution of the traditional risk management, and it has tried to solve all the precedent challenges providing a better risk-return decision making process (Fraser and Simkins, 2011). Therefore, the Enterprise Risk Management approach, considers all the risk areas as a part of a unique, integrated and enterprise-wide system, and simultaneously, it provides a wide variety of techniques for analyzing and managing risks in a more holistic way with a double extent of assimilating the new risk approach in the corporate culture and enhancing company value (Fraser and Simkins, 2011). Finally, the ERM has extended the range of risks considered in the analysis, including operational risks together with strategic and financial risks (Segal, 2011).

With the introduction of the revised ERM model, the analysis of operational risks was completely reviewed and implemented for having a better response to this wide variety of risks in continuous expansion (Franklin, 2008). The operational risks are the third category of risks introduced by Basel II in 2009 with the two previous ones: financial risks[5] and strategic risks[6] (Segal, 2011).

The most common definition of operational risk is the one used in Basel II framework:

---

[3] Def Risk Appetite: it is the level of risk a firm is willing to accept in order to meet its strategic objectives (Segal 2011).

[4] Def Risk Exposure: it is the quantified loss potential of a business. It is usually calculated by multiplying the probability of an incident occurring by its potential losses (Segal 2011).

[5] Def of financial risks: a category of risks related to unexpected changes in external markets, rates, prices and liquidity supply and demand (Segal, 2011).

[6] Def of strategic risks: a category of risks concerning unexpected changes in key elements of the strategic formulation of execution (Segal, 2011).

"*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risks" (*BCBS, 2006).

This means that operational risks are a category of risks related to unexpected changes in elements related to company operations, as human resources, technology, processes and disasters. Basel II has also introduced a new capital requirement for operational risks that is fundamental for the operational risk modelling (Rippel and Teply, 2010).

Table 1. All types of operational risks.

Risks	Description
Technology	Technological instruments are not performing as expected. This means problems in data security, data privacy, data integrity, capacity and reliability of the It system.
Litigation	Unexpected civil suits or judgments against the company.
Compliance	The level of compliance is not adequately matching regulators expectations.
External Fraud	Unexpected fraud made by external parties.
Disasters	They are unexpected natural or man-made disasters, divided in several types such as weather related (hurricanes), health related (pandemic), accidental (fire), general act of destruction (war, terrorism, rioting) or specific act of distraction (sabotage), and environmental damages.
Human resources	A loss in terms of performance related to human resources such as the loss of key personnel, unexpected changes in talent management, productivity and conduct.
Processes	They are not functioning as expected.

Source: Segal S. (2011), "Corporate Value of enterprise Risk Management: the next step in Business management", Wiley Corporate F&A, chapter 1.

There are three different approaches which has been set by Basel II in order to calculate operational risks:

1) Basic Indicator Approach;

2) Standardized Approach;
3) Advanced Measurement Approach (Rippel and Teply, 2010).

Basically, these three techniques are part of two broad categories for quantifying operational risk: top-down approach and bottom-up approach. The first one, is based on the quantification of operational risks without attempting the specific events or causes of losses; on the contrary, the second one applied a micro level analysis based on the identification of internal events for the calculation of the operational risks. The former includes tools such as the Risk Indicator Model, which relays on numerous series of operational risk indicators to track the above-mentioned risks, and the Scenario Analysis and Stress Testing models based on an analysis of multiple possible situations (what-if scenarios). Instead, the latter approach considers actuarial types of model based on two components, frequency and loss severity distributions, in order to model the data sample for historical risk losses (Rippel and Teply, 2010). The A.M.A. is still today the most sophisticated approach used for the quantification of operational risks, also because it satisfies several modelling assumptions essential for the risk management analysis. Observing historical data is a basic step for the prediction of future losses and the observation period of internal loss data must be at least of five years in order to improve the operational risk measures (Embrechts, Furrer and Kaufmann, 2003). Data for the analysis on operational risks can be collected either by internal sources, coming from the inside of the organization, more likely provided by managers during their activity of running the business, after a verification of actual operational losses in company value, or by external sources through vendors' activities who gather data for the company in operational losses have occurred (Chaudhuri and Ghosh, 2016). Moreover, according to the new framework of Basel II, these quantitative data are mixed with experts' opinions with the goal of creating a general model that can be implemented in several fields (Franklin, 2008).

Basel II has also implemented a new model called "Advocacy Model", that combine quantitative data with the qualitative experts' opinions for a more complete analysis of all the available information. This methodology for evaluating operational risks is particularly appropriate for modelling extreme risks in specific areas such as terrorism, biosecurity and natural disasters (Franklin, 2008). It is named "extreme risk", a risk that is related to a specific event that may happen very rarely or even never. Such events are extremely rare, and this means that they are usually outside the range of critical events considered in the risk management analysis, moreover there are few or no reliable and representative data of their

probability distribution (Franklin, 2008). Therefore, the evaluation of extreme risks is particularly difficult and different from the standard approach used for the calculation of the impact of other types of risks, mainly focused on choosing a model for the description of quantitative problems, selecting the right parameters considering the data available, and at the end, employing the resulting statistical model for making predictions (Franklin, 2008). Instead, the extreme events' probability must be evaluated considering several sources of evidence and combining them because they are not useful and reliable in isolation, underling the importance for a better integrated approach[7] for implementing this activity. Therefore, data came from several sources such as experts' opinions, scientific knowledge linked to the case and commonsense knowledge. Risk management does not provide an established methodology in order to compute and elect the statistical probabilities which arise from the pre-mentioned sources (Franklin, 2008). Finally, it is crucial to not neglect any source of evidence or possible interpretation, especially in situations in which data are scarce, otherwise there is a high possibility to have an uncorrected extreme risk valuation that can lead to an increase of avoidable costs. The extreme risk valuation structure can be exported and used to all fields that involve the presence of extreme risks (Franklin, 2008).

1.2.2 Definition and characteristics of Disaster Risks.

A disaster happens when an extreme natural event arises striking a vulnerable[8] society. The final impact of the natural event strictly depends on the characteristics of the society considered, such as politics, economics, structure of the social community and environment (BMZ Report, 2015). Therefore, disasters may seriously affect citizens and communities destroying temporarily and sometimes even for many years, the livelihood security of their members (Baas, Ramasamy, Dey de Pryck, and Battista, 2008). Three elements combined together can lead to a disaster:

1) Hazard Risk Conditions;
2) Vulnerability of the society;

[7] A better integrated approach is one of the main characteristics of the new Enterprise Risk Management especially introduced because of the terroristic attack of September 11th (Segal, 2011).

[8] Def of vulnerability: "the conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards" (Baas, Ramasamy, Dey de Pryck, and Battista, 2008).

3) Limited capability of the community to reduce the negative impact of the hazard.

The first step for avoiding disasters is the recognition of possible vulnerabilities in the community's risk context and following the enhancement of people's strengths in order to mitigate the impact of hazards (Baas, Ramasamy, Dey de Pryck, and Battista, 2008). It is fundamental the existence or absence of a well functioned institutional and socio-economic system specifically created for the mitigation and prompt response to hazards because it determines the level of adaptability of a community to the impact of unexpected extreme events (Baas, Ramasamy, Dey de Pryck, and Battista, 2008).

In order to have a better control over hazards (natural[9] or man-made) and disasters, a precise Disaster Risk Management was implemented. Its aim is reducing the vulnerability of communities to extreme natural events, so in case these events occur, they won't result in terrible disasters. This is related to the concept that extreme events cannot be easily predicted, for that, the only way is to find a method for mitigate the consequences (BMZ Report, 2015).

Hazards and disasters are the principal elements analyzed by the Disaster Risk Management model, and they both have clear definitions and terminologies:

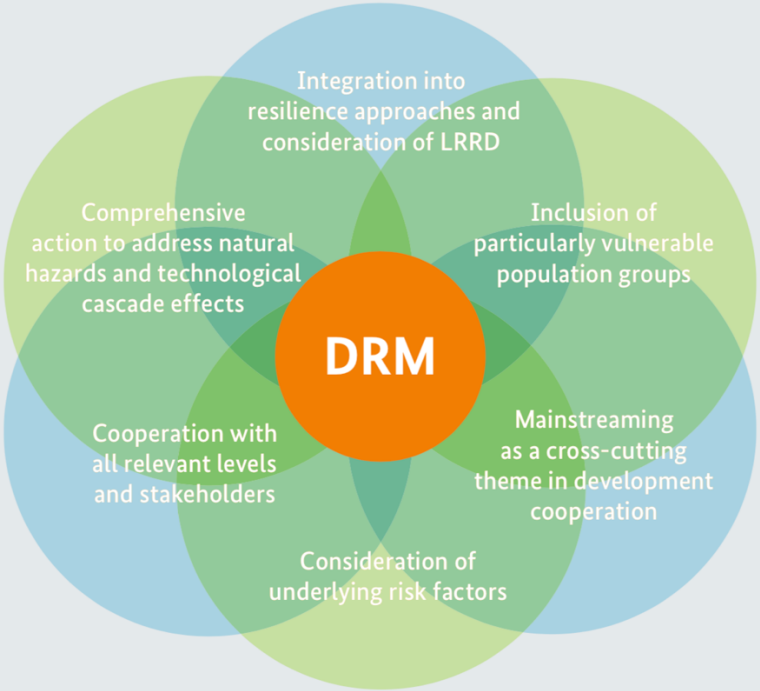
1) Hazard**:** "a potentially damaging physical event, phenomenon or human activity that may cause the loss of life or injury, property damage, social and economic disruption or environmental degradation" (Baas, Ramasamy, Dey de Pryck, and Battista, 2008).
2) Disaster**:** "it is a serious disruption of the functioning of a society that causes material, human, economic and environmental losses that exceed the ability of the affected society to cope using its own resources" (Baas, Ramasamy, Dey de Pryck, and Battista, 2008). It is a function or the risk process, resulting from the combination of three different elements: hazards, vulnerability conditions and inability to reduce negative consequences of the extreme event.

Disaster Risk Management (DRM) is a broad concept that goes beyond the precedent Disaster Risk Reduction (DRR) model, which is just a conceptual framework made by several elements with the specific aim of minimizing vulnerabilities and disaster risks throughout the society, thanks to numerous actions of prevention and mitigation of the

[9] Types of natural hazards: they can be classified according to their geological (earthquake, tsunami, volcanic activity), hydro-meteorological (floods, storms, drought) or biological (epidemic) origins (Baas, Ramasamy, Dey de Pryck, and Battista, 2008).

impacts of these hazards in order to develop a sustainable development[10]. Indeed, DRM adds a new management vision base on the relationship between mitigation, prevention and preparedness of response (Baas, Ramasamy, Dey de Pryck, and Battista, 2008). For that, it can be defined as a complex and continuous process of planning and implementing adapting strategies and methodologies that involves physical and non-physical measures for the analysis and mitigation of disaster risks with the scope of reducing hazards and vulnerabilities and reinforcing adaptation capacities of individuals and communities (BMZ Report, 2015).

Figure 1. Success factors of an effective Disaster Risk Management.



Source: BMZ Report (June 2015), "Disaster Risk Management: Approach and Contributions of German Development Cooperation", Federal Ministry for Economic Cooperation and Development (BMZ), pp. 6.

It is particularly important the link between DRM and the concept of resilience; it can be defined such as the capacity of people, communities and institutions to withstand acute negative shocks or chronic stress caused by different situations (crises, extreme natural

[10] Sustainable development is defined as "Development that meets the needs of the present without compromising the ability of future generations to meet their own needs" (Baas, Ramasamy, Dey de Pryck, and Battista, 2008).

events or violent conflict) and to adapt in order to recover in a short time maintaining a sustainable development without compromising long-term prospects (BMZ Report, 2015). Linking Relief, Rehabilitation and Development approach (LRRD) must be integrated with resilience approaches with the aim of linking short-term relief measures with longer-term development programs that permits the creation of valuable synergies which provide a much more sustainable response to crisis situations (BMZ Report, 2015).

As previously said, there are several factors that must be analyzed in order to create an appropriate framework for DRM, in particular they could be divided in four broad categories of risk factors:

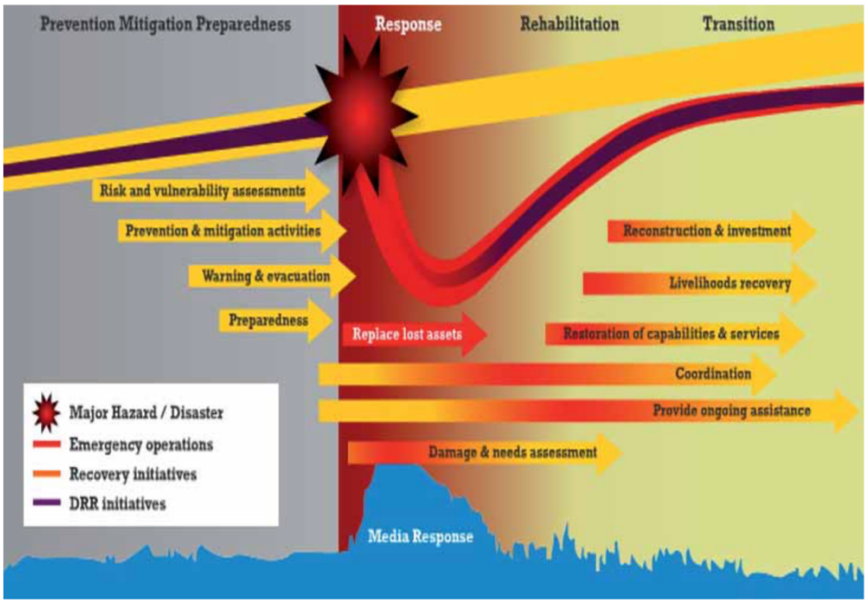
1) Effect of climate change: this gradual change in atmospheric conditions is leading to global warming and so it is negatively affecting ecosystems. Natural catastrophes such as floods, storms and droughts are become more and more frequent (BMZ Report, 2015);
2) Poverty: it is a factor that tremendously increases the vulnerability to negative shock, in fact, almost the seventy per cent of deaths resulting from disasters are concentrated in less developed countries. These people are forced to live in places particularly exposed to destructive natural events, diseases and crimes (BMZ Report, 2015);
3) Fast process of urbanization: poor urban infrastructures are a problem that afflict especially people now living in developing countries. The land tenure in uncertain and the quality of life is very low, moreover the spread of disease is very rapidly and lethal in these particular environments (BMZ Report, 2015);
4) The rise of conflicts and violence: in the world more than 1.5 billion people live in unsafe, fragile and conflict-afflicted countries, moreover weak institutions reinforce this spiral of violence (BMZ Report, 2015).

In addition to these factors, catastrophic (disaster) risks are usually based on two characteristics: fat tails and correlated losses. Fat tails means that the probability of a catastrophic event slightly decline in relation with its severity; the higher the severity is, the lower the probability. These specific risks are also correlated in space, the higher is the concentration of people and buildings in the same area and the higher will be the number of victims. Therefore, geographical proximity is a very important factor that must be considered in the estimation of total damages made by catastrophic events (Kousky, 2011).

The DRM framework is particularly valuable because it promotes a new and improved holistic approach in the valuation of disaster risk and in addition because it demonstrates the

existence of a relation between disaster and development, in which activities such as mitigation and prevention play a key role for obtaining a sustainable development of communities (Baas, Ramasamy, Dey de Pryck, and Battista, 2008).

Figure 2. Revised Disaster Risk Management Framework (DRMF).



Source: Baas S., Ramasamy S., Dey de Pryck J., Battista F. (2008), "Disaster risk management systems analysis: a guide book", Food and Agriculture Organization of the United Nations, pp 7.

This framework states the importance of ongoing development activities in the treatment of disasters, which start with the preparation of prevention and mitigation actions, and in case of emergency, the focus in on responsiveness actions, recovery and rehabilitation through a phase of transition until the pre-disaster level of wealth is finally reached. Tre transition between pre, during, and post disaster circumstances is fluid especially in countries regularly exposed to catastrophic events with well functioned DRM systems (Baas, Ramasamy, Dey de Pryck, and Battista, 2008).

Disaster Risk Management framework appears to be fundamental in the analysis of the impact and consequences of disasters on Micro, Small, Medium and Large enterprises. Indeed, the restoration of the socio-economic wealth of the community is a key step for firms' recovery and at the same time, because firms contribute to the well-being of their societies by providing capital, employment, goods and services, their rehabilitation is closely correlated to community's restoration (UNISDR Report, 2013). MSMEs[11] are more affected by disasters than large enterprises, because the latter one has access to a wide range of coping

[11] MSMEs: acronym of micro, small and medium enterprises.

strategies. On the contrary, MSMEs have a limited set of risk-management techniques they can access and moreover, if they are active in developing countries, there are additional factors which can lead to the exacerbation of their vulnerabilities (lack of compliance with rules and norms, lack of social protection for workers, informality of relationship with institutions and firms…). All these elements basically lead to a conspicuous loss of assets, supplies and customers in case of crisis situations, mining the surviving strategies of MSMEs (UNISDR Report, 2013). On the other hand, small-medium firms possess a higher flexibility than bigger ones due to their lower level of capital needed for operations, and this advantage can be exploited after disasters for mainly supporting a faster and equitable rehabilitation of local communities. MSMEs appear to be the engine of local socio-economic recovery through the reconstruction of infrastructures and by stimulating local employment and production, while the effect of the catastrophe is redistributed to a larger scale level, usually supported by governmental recovery plans (UNISDR Report, 2013). The main pros of central Governments' recovery actions are the robust budget in term of resources they can leverage and their ability to coordinate and involve in the reconstruction process various stakeholders, such as international institutions, private sector and regional or local Governments. It is their primary responsibility to support the social and business environment in becoming stable again after a situation of crisis (UNISDR Report, 2013).

1.3 History, definition and tactics of Terrorism

The section is focused on giving a definition, describing the history and analyzing the different forms of terrorism. It is divided in three sub-sections which give a deep explanation of the overall concept of terrorism. The first section illustrates the principal difficulties in giving a univocal definition of terrorism and the changes happened in terrorism's history. Sub-section two elucidates the ten types of terrorism together with the five main strategies and goals pursued by terroristic organizations. Finally, sub-section three defines the Global Terroristic Index and successively illustrates the most important terroristic groups and the deadliest terroristic attacks in the world history.

1.3.1. Definition and history of Terrorism.

The events of September 11th have put emphasis on the concept of terrorism by giving the duty to institutions and Governments to better understand and predict this phenomenon in

order to avoid tragedies such as the previous mentioned (Mannik, 2009). The first task of Governments is to correctly define what terrorism is; it is very complicated to give just one universal definition of terrorism but at the same time it is absolutely necessary for the development of a consistent framework for understanding and dealing with this increasing phenomenon (Mannik, 2009). Today there are almost one hundred different definition of terrorism, but the most common one is the UK Terrorism Act definition created in 2000 that explicitly specifies the characteristics that an action has to possess in order to be classified as terrorist attack (Roser, Nadgy and Ritchie, 2016):

"the use or threat of action designed to influence the Government or an international governmental organization or to intimidate the public, or a section of the public; made for the purposes of advancing a political, religious, racial or ideological cause, and it involves or causes:

1) Serious violence against a person;
2) Serious damage to a property;
3) A threat to a person's life;
4) A serious risk to the health and safety of the public; or
5) Serious interference with or disruption to an electronic system (Roser, Nadgy and Ritchie, 2016)".

The scope of having a universal definition is crucial for coordinating the international collaboration between countries and having a quick response to terroristic attacks. In addition, without a clear definition that answer the question of "what terrorism is", any duties or responsibilities can be charged on countries that support terroristic groups or they are involved in state terrorism, nor any actions can be taken to fight terroristic organization and their allies (Mahmood, 2002). Having a universal definition is a great achievement that can improve several factors:

1) International cooperation and military operations in order to fight against terrorism and ensuring the highest effectiveness of anti-terroristic practices;
2) Actions against states that sponsor terrorism for obtaining military support from terroristic organization with the scope of increasing their power and subjugating the population;
3) Legislative and Punitive actions where a clear definition is fundamental for making specific laws created to prohibit terrorism and to provide assistance to people who experience it;

4) Distinguish terrorism from freedom struggles which possess a measure of legitimacy among nations (Mahmood, 2002).

For all the previous mentioned reasons several codes where developed by different states for defining terrorism: United States and European Union have their own code (Mahmood, 2002).

The word "terrorism" came from the Latin term "terrere", which actually means "to frighten". The word was first used in the contemporary era during the Reign of Terror in France between 1793-1794 with Maximilien Robespierre as the leader of the country. He specifically describes terror as "…nothing more than justice, prompt, severe and inflexible justice…; it is a consequence of the general principle of democracy applied to our country's most urgent needs" (Mannik, 2009). There are several modern examples of state terrorism in the last one hundred years: Nazi Germany, Stalinist Soviet Union, the communist China of Mao Zedong, and numerous others less famous totalitarian regimes or dictatorships (Mannik, 2009). Scholars have identified four different waves of terrorism, and each one has its own specific characteristics, supporters and modus operandi and each one last at least few decades. The first one started in the 1880s, called the Anarchists Wave focused on the fight of totalitarian regimes such as the Russian one and it spread rapidly to all Europe, Asia and America (Simus, 2016). It lasted for almost 40 years and it was a period in which violence and propaganda increased tremendously because of the inventions of bombs and rotary press. Terrorists were inspired by the French Revolution, for that political targets where hit to shake public opinion (Simus, 2016). The second wave called Anticolonial Wave began in the 1920s and it was different from the first one because they have learned that assassinating political figures was counterproductive and for that terroristic attacks were focused on the elimination through assassination of police officers (Government's eyes and ears). The third one began in 1960s it was called New Left Wave and it gradually fade out in the 90s leaving just few restricted groups active in Spain, France, Perù and Columbia (Simus, 2016). In that occasion, radicalism was often linked with nationalism, like In the Basque Nation and Liberty (ETA[12]) and the Armenian Secret Army for the Liberation of Armenia (ASALA[13]);

[12] ETA is the acronym of Euskadi Ta Askatasuna, which was a terroristic organization whose scope was the independence of Basque Nation from Spain. It was disbanded in 2018.

[13] ASALA was an Arminian military organization that operated between 1975-1990s with the scope of forcing the Turkish Government to publicly admit its responsibility for the Armenian Genocide in 1915.

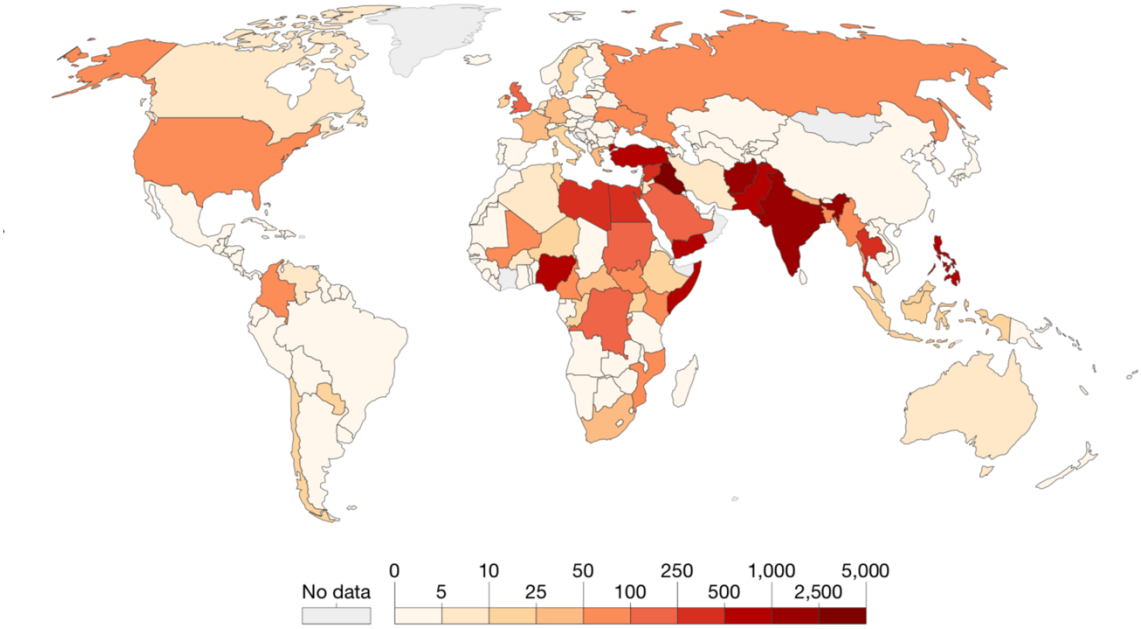
kidnapping and hostages taken were very numerous during that decades (Simus, 2016). The last wave is called Religious Wave and it officially began in 1979, in the same decades of the third one, but it is still running today. In previous waves religion was also an important factor but the aim of terrorists was to create sovereign states, therefore religion was just means to obtain this final goal. Instead, in the fourth wave religious identity had a completely different significance, indeed it was used, and it is still used, to justify terroristic attacks and as an instrument used to create new principles for a new incoming world (Simus, 2016). Islam is the most significant religion of this wave, but it is not the only religion that creates terrorists: in Punjab, the Khalistan Movement arose as a Sikh separatist movement with the aim of creating a separate country and it was involved in several terroristic attacks, with the most famous one was the tragic death of 329 people on Air India Flight 182 after the explosion of a bomb in 1985. In 1995, Aum Shinrikyo, a terrorist group that followed different religious movement (Buddhism, Christianism And Hinduism), released nerve gas on the Subway of Tokyo killing twelve people and injuring almost 3000 (Simus, 2016). The fourth wave has introduced a new and deadly tactical innovation called suicide bombing in which martyrdom is considered as the maximum apt of faith for the religious cause. Terroristic groups have made much more massive attacks than other waves, against military and governmental institutions, and they particularly hit Americans which became a frequent target. During this period the Al Qaeda led by the Saudi Osdama Bin Laden was built with the aim of creating a single state for all Muslims governed by the Islamic Law Sharia (Simus, 2016). At the end, the massive attack on September 11th, coordinated by this organization, was a turning point in the war on terror; several changes and heavy investments were globally made in order to avoid another similar catastrophe, moreover military intervention became necessary especially in those countries in which the most important terroristic groups were active (Simus, 2016).

1.3.2 Types of terrorism: goals and strategies.

The attack of 11 September 2001 was the most relevant terroristic attack in the world history and it has allowed the beginning of the "War on Terror", a war fought against terrorists and their murderous ideology (Mannik, 2009). In the short term, this war is focused on coordinate military operations for killing or capturing terrorist leaders in order to prevent other future attacks, but in the long run, it is actually a battle of ideas with the only scope to eliminate terrorists' own distorted version of religion, which gives them the justification for

murdering innocent people that are considered non-believer (Mannik, 2009). The War on Terror had led to the subsequent military occupation of Afghanistan in 2001 and Iraq in 2003, considered as the two countries where terrorists' headquarters were located (Roser, Nadgy and Ritchie, 2013). The event of September 11th has also led to a shift in the concentration of global terroristic activities, indeed, the most critical attacks were mainly concentrated in Muslim countries due to their radical and extreme Islamic ideologies and their persistence use of violence to intimidate people (Roser, Nadgy and Ritchie, 2016).

Figure 3. Number of Terrorism attacks in 2016.



Source: Roser M., Nadgy M., Ritchie H. (2013), "Terrorism", Our World in Data, pp. 5.

The main evidence in the number of terroristic attacks happened in 2016 is that the higher concentration of terrorism's tragic events is in countries where the majority of the population profess Islamism or Hinduism, such as Middle East, North Africa, India and Pakistan. It is consistent change from past trends that has experienced a higher concentration of terroristic attacks in Latin America and Central Africa. In particular, Iraq is most damaged country in which almost 5000 terroristic attacks took place in 2016 (Roser, Nadgy and Ritchie, 2016).

During the last twenty years, terrorism has been studied in all their forms in order to have a better and more functional knowledge that can assist Governments and international institutions in preventing and mitigating this complex and dynamic phenomenon. From this analysis it has emerged several forms of terrorism, each one with commune and own specific

characteristics, with different modus operandi and with certain areas or countries in which attacks take place (Mahmood, 2002).

Ten types of terrorism have been identified:

1) State Terrorism: it is the use of violence by states to accomplish political goals and for the repression of their own citizens, mainly used by Israeli and Indian Government;
2) State Sponsored Terrorism: they are terrorism action launched and sponsored by a country against another nation with the systematic use of violence and military forces with the ultimate goal to achieve long term strategic or political aims. Several countries such as Cuba, Libya, Iraq and North Korea were accused to support terrorists;
3) Nationalist Terrorism: it is a form of terrorism that tries to create a separate state for their specific national group by the use of terroristic attacks, by drawing attention to war for national independence and liberation;
4) Religious Terrorism: it is focused on the use of violence for servicing distorted religious purposes usually targeting people that are considered non-believer and so not member of the terrorist's religion. The most important organization of this type of terrorism is Al Qaeda;
5) Left Wing Terrorism: its aim is to destroy capitalism and replace it with socialist or communist regime;
6) Right Wing Terrorism: it is the contrary of the Left-Wing terrorism, in fact, terroristic actions have the goal to eliminate and successively substitute liberal democratic Governments with fascist states;
7) Anarchist Terrorism: this type of terrorism is aimed at the achievement of consistent changes in governmental policies on particular problems or ever to overthrow established Governments;
8) Suicide Terrorism: defined like politically motivated violent attack made by a single person who causes his own death in order to kill his chose target;
9) Cyber Terrorism: activities of hacking and other computer resources in order to intimidate, damage and coerce other people or Governments;
10) NBC Terrorism: this is the most dangerous type of terroristic attack because it uses weapons of mass destruction, such as nuclear bombs, chemical and biological weapons, to destabilize Governments and acquiring more and more power and

creating fear among people. An attack of this type can create enormous damages to humans, man-made structures, environment and even the biosphere (Mahmood, 2002).

International entities have also deeply analyzed the main strategies that terrorists applied to achieve their goals (Kydd and Walter, 2006). Usually, they are too weak to impose their will directly, for that, they use specific strategies based on persuading target audience's perception to accomplish their wishes by altering their believes giving a sense of legitimacy to their actions, imposing a degree of commitment to their cause of their determination, and finally established a good and transparent communication of their intents with people, with reasonable and precise goals to reach (Mannik, 2009). There are five principal strategies implemented in terroristic campaigns (Kydd and Walter, 2006):

1) Attrition;
2) Intimidation;
3) Provocation;
4) Spoiling;
5) Outbidding.

The first one, attrition, is used to convince the enemy that terrorists are powerful enough to seriously damage the enemy if he doesn't stop a particular policy or activity (Kydd and Walter, 2006). Instead, intimidation is a strategy that try to persuade the population that terrorists are stronger than government, so they can punish disobedience and no institutions can stop their actions. If the pre-mentioned strategy is well implemented, people will start to behave as terrorists want. The third one, provocation, is an effort on inducing the enemy to respond to terrorism actions with other violent initiatives, and by acting like this, it involuntarily moves people to support terroristic causes (Kydd and Walter, 2006). Spoiling strategy scope is to avoid a peace overtures between target government and moderate leaders of terroristic organizations. It is a strategy based on mistrust between the two factions and it finally succeeds when the parties fail to implement a peace agreement (Kydd and Walter, 2006). The last strategy is called outbidding, and it arises only when two or more parties are competing at the same moment for the control of an area, and when population is uncertain about which factions best represent and protect their interests. In this case, the strategy is successful only if terrorists are able to convince the population that they possess a stronger capacity to resolve conflict and protect people's interest compared to other rival groups, therefore they deserve population support (Kydd and Walter, 2006).

The terroristic strategies' analysis was fundamental for creating a model in order to better understand which type of strategy is implemented to accomplish different goals (Mannik, 2009). Scholars and governmental agencies have defined five different goals in line with the previous mentioned strategies:

1) Regime change;
2) Territorial change;
3) Policy change;
4) Social control;
5) Status quo maintenance (Mannik, 2009).

The first goal aimed at the overthrow of the previous government by replacing it with another one that is controlled by terrorists or at least that is more in line with terrorism objectives. Territorial change means completely eliminate the presence of the state on a specific territory by cutting all the economic and social relationship with it, in order to create a new state or to join another already existing state (Kydd and Walter, 2006). The third type, policy change, is a vast category made by different strategies applied for changing policies implemented by a government in a specific country and for forcing other states to cut their support to terrorists' enemies. Particularly famous was the Al Qaida's request to the United States to stop supporting Israeli military actions (Kydd and Walter, 2006). Contrary to the previous strategies, social control is focused on the oppression and constant supervision of the behavior of individuals, rather than government policies. The last strategy, the status quo maintenance, is specialized in giving strong support of already existing regimes (usually a totalitarian regime or a dictatorship) in order to defeat political groups that want to change them (Mannik, 2009).

1.3.3 Global Terrorism Index: deadliest terroristic attacks in history and most important terroristic groups.

A more comprehensive study of the terrorism phenomenon was required in order to prevent catastrophes as September 11th. For this purpose, the Global Terrorism Index (GTI)[14] was developed thanks to the collaboration of several governmental agencies from almost all countries in the world (Institute for economics and Peace Report, 2017). The Global

[14] GTI is a very accurate report published annually by the Institute for Economics and Peace. Its research is focused on key global trends in terrorism since 2000.

Terrorism Index is a thorough analysis that considers direct and indirect impact of terroristic actions in 162 states in terms of property damages, number of killed persons, number of injuries and psychological effects that terrorism has on population. This research covers the 99,6 per cent of the world's citizens (Institute for economics and Peace Report, 2017). The GTI obtains its data source about terrorism from the Global Terrorism Database (GTD), which is created and managed by the National Consortium for the Study of Terrorism and Response to Terrorism (START)[15], that composes an accurate score in order to rank every nation according to terrorists' activities on its territory. The GTD is a systematically and comprehensive analysis that collects data from domestic and international terrorist incidents including more than 140.000 cases (Institute for economics and Peace Report, 2017).

The Global Terrorism Database has noticed a specific relation between the growth of terrorism and two different variables: information and type of regime (Kydd, Walter, 2006 and Mannik, 2009). There is an inverse relation between information and terrorism; the lower is the availability of information and the higher it the growth possibility of terrorism (Kydd and Walter, 2006). This is briefly explained by the fact that in an uncertain environment, where there is no transparent communication between citizens and governments, it is easier for terrorists to manipulate population's behavior (Kydd, Walter, 2006 and Mannik, 2009). Therefore, the fight against terrorism may be thought as a continuous struggle to collect and spread reliable information in countries full of uncertainty (Kydd and Walter, 2006). The second variable, the regime type, is a study about which form of government is more sensitive to terroristic attacks and facilitate the spread of terroristic groups on the territory (Kydd and Walter, 2006). The analysis suggests that democracies are far more sensitive to terrorism that totalitarian regimes, moreover they possess structural characteristics that make them an attractive target for terrorists' attacks (Kydd and Walter, 2006).

The regional overview of terrorism activities underlines that the vast majority of attacks has occurred in the Middle East and North Africa, South Asia and sub-Saharan Africa regions (Institute for economics and Peace Report, 2017). These regions account for the 84 per cent of the total number of attacks happened in 2017 and 94 per cent of total deaths. On the other side, Caribbean and Central America are the safest regions in the world considering the

[15] START is a research and education center focused on learning the different causes and consequences of terrorism in the USA and around the world. It was launched in 2005.

number of terroristic attacks, less than 0,05 per cent of the total (Institute for economics and Peace Report, 2017). Ten countries were ranked as the more targeted and damaged by terrorism in 2017 and more in general in the last five years:

1) Iraq
2) Afghanistan
3) Nigeria
4) Syria
5) Pakistan
6) Yemen
7) Somalia
8) India
9) Turkey
10) Libya

In these nations, a vast range of terroristic groups are active, but the Global Terrorism Database has identified four major organizations that are responsible for more than 70 per cent of all deaths and attacks made by terrorists: ISIL, Boko Haram, Taliban and Al Qaida (Institute for economics and Peace Report, 2017). ISIL, the Islamic State of Iraq and the Levant, is the most dangerous and active group of the last years. This group is active in several areas; therefore, the location of their attacks can vary from Europe, Middle East, North Africa and South Asia (Institute for economics and Peace Report, 2017). They have caused more than nine thousand deaths and almost eight thousand injuries, where more than half of the attacks were concentrated on private citizens and property and suicide bombings were the most common technique used with the highest date rate (Institute for economics and Peace Report, 2017). The second group, Boko Haram, an Islamic group originated in northern Nigeria but successively spread in neighboring countries such as Cameroon, Chad and Niger. In 2014 it was the most dangerous and deadliest terroristic group but during the last years it has suffered consistent defeats because of significant military actions implemented by Multinational Joint Task Force (Institute for economics and Peace Report, 2017). In 2016, Boko Haram split into three separates factions with different strategies; one of these factions is aligned with ISIL interests and therefore it conducts terroristic attacks through suicide missions focused on hitting civilians (Institute for economics and Peace Report, 2017). The Taliban organization arose in Afghanistan in 1994 as a reactionary group with aim of taking control of the country and successively declaring it an Islamic emirate guided by their leader as head of the state (Institute for economics and Peace Report, 2017). With the NATO invasion in 2001, this group has experienced several difficulties and defeats, but it is still today one of the most active terroristic organizations. In 2017, the number of deaths caused by their actions has risen to more than 3,5 thousand people with almost the same number of people injured. This group is mainly engaged in traditional armed conflict

for defeating Afghan National Guard, focusing all their military forces on territorial control (Institute for economics and Peace Report, 2017). The last terroristic group, Al-Qaida, was formed in 1988 by Usama bin Laden with the extreme goal to expel all Western military forces from Middle Asia. In order to reach their goals, the organization has coordinated large scale terroristic actions which have been culminated with 11 September 2001 attack. Al Qaida has created a decentralized structure that allows regional affiliates to independently operate without the group leadership. Therefore, even if they are active in different areas, they implement the same method of attacks, primarily bombings and explosions, which in 2017 accounts for more than two thousand deaths, and the majority of them were civilians (Institute for economics and Peace Report, 2017).

Table 2. The 10 worst terroristic attacks in terms of insured losses.

Description of the event	Location	Date	Property damages	Fatalities
Hijacked airlines crash into the World Trade Center, Pentagon and rural area of Pennsylvania	New York, Washington, Pennsylvania; USA	September 11, 2001	32,5 billion dollars	2996 people
Bombs explodes near NatWest Tower	London, UK	April 24, 1993	1,2 billion dollars	1 person
Irish republican Army car bomb explodes near a shopping center	Manchester, UK	June 15, 1996	980 million dollars	None
Bomb explodes in the London's financial district	London, UK	April 10, 1992	883 million dollars	3 people
Bomb explodes in the garage of the World Trade Center	New York, USA	February 26, 1993	822 million dollars	6 people
Group of rebels destroy 3 airliners, 8 military aircraft and seriously damage e civilian aircraft	Colombo, Sri Lanka	July 24, 2001	525 million dollars	20 people
IRA bomb explodes in South Quay Docklands	London, UK	February 9, 1996	341 million dollars	2 people
Air India Boeing 747 was destroyed by a bomb	Over the North Atlantic	June 23, 1985	212 million dollars	329 people

A bomb seriously damages the federal building of Oklahoma City	Oklahoma City, USA	April 19, 1995	192 million dollars	166 people
Explosion of hijacked Swiss aircraft	Zerqa, Jordan	September 122, 1970	167 million dollars	None

Source: Hartwig R. P. (2008), "Terrorism & Enterprise Risk Management: Scenarios & Uncertainty", Enterprise Risk Management Symposium

Table two specifies the most significant terroristic attacks in world history in terms of property damages. It is divided in five columns where a description of the main event is given, within the date and the location. The last two columns show the number of fatalities and express the entity of the damages in terms of million or billion dollars. From the analysis, it is evident that the major incidents have taken place in two specific countries: United Kingdom and United States. Finally, the table show the significant difference of September 11th damages compared to the others (Hartwig, 2008).

1.4 Terrorism Risk: a new challenge for the insurer

The section is focused on the analysis of terrorism risk and its relationships with the modern society, also called risk society. It is divided in two sub-section, where the first one firstly examines, the risk society and its characteristics, giving a precise definition of the concept of security and precautionary risk, and secondly it investigates on the changes happened in the modern society during the last decades, briefly explaining the relevant relationship between terrorism and risk society. On the other hand, sub-section two is focused on the introduction of terrorism risk, which is the principal topic of chapter two. In particular it explains the difficulties in hedging against terrorism risk, its features and new measures applied for better prevent this threat.

1.4.1 Definition of risk society and its relationship with terrorism risk.

The incident of September 11th has strengthened the idea that we are now living in global risk society. It is a concept strictly related to the numerous changes happened in the modern era and it is defined by the German sociologist Ulrich Beck as "the systematic way of dealing with hazards and insecurities induced and introduced by modernization itself" (Beck, 2002). The speeding up of modernization and the dynamic nature of the modern risk society have

produced a large gap between quantifiable risk and non-quantifiable ones that have underlined the importance of controlling these new types of risk. Basically, there are at least three different and unquantifiable threats in the world risk society: ecological problems, recurring global financial crises and the rising of terrorism organizations (Beck, 2002). These global risks are unequally distributed in the globe; therefore, they result particularly difficult to prevent and to successively mitigate their consequences. They impose a moral duty on governments to protect individuals' right of security and this means the obligation to control such threats in order to avoid catastrophes which can jeopardized world population's well-being (Wolfendale, 2006). Anyway, there is a clear difference between the first two types of threats and terrorism, the third one. Ecological and financial risks clearly result from issues in the accumulation, management and distribution of goods[16], because of bad but unintentional decision taken by the society. On the contrary, terroristic activities are intentional bad actions with the aim of producing fear and socio-economic crises and simultaneously damaging people security (Beck, 2002).

Security is today one of the most important things that the world risk society must provide to their citizens, together with freedom, democracy, moral and social values and appropriate living standards (Wolfendale, 2006). Even if there is no clear definition of security, the most common and accepted is the one proposed by Baldwin that define security in reference to "… the actor whose values are to be secured, the values concerned, the degree of security, the kinds of threats, the means for coping with such threats, the cost of doing so, and the relevant time period" (Baldwin, 1997). Therefore, he underlines that security can only be defined negative, when there is the absence of threats against life, bodily integrity, health and property (Baldwin, 1997). As previously analyzed, there are several manners in which national and individual security can be threaten: from natural disasters, diseases, wars, crimes, financial crises, to terroristic incidents. All these factors can seriously damage the territorial integrity of a state and weaken its ability to provide security's services to its population (Wolfendale, 2006). This is the main explanation why a new form of governmentality was developed in the last decades, based on strategies of surveillance, injunctions to integration, much more sophisticated and continuous precautionary actions and exacerbate policies against anti-social behavior (Aradau and Van Munster, 2007). As a consequence, the advent of the risk society has led to the arise of a precautionary element

[16] The word goods in this case is used for explaining a more general concept that includes production and consumer goods and also capital and financial instruments.

which has in turn guided to new configurations of risk management that mandatorily required to avoid at all costs possible disastrous prospectus of the future (Aradau and Van Munster, 2007).

All the technological and industrial progresses made in twentieth century has led to a complex situation where the prediction of all kind of risks is no longer a possible option as a result of the enormous growth happened. In the modern society, risk is a very difficult factor to predict, either because a multitude of risks flourish continuously, either because they are usually inter-correlated and difficult to analyzed in isolation (Aradau and Van Munster, 2007). Beck himself define the concept of risk as something that comes from the systematic way of dealing with uncertainties and hazards created by modernization itself (Beck, 2002).

The analysis of these catastrophic risks developed in the modern era, from economic crisis, to environmental catastrophes, until terrorism, has underlined the necessity to change the approach that the risk society must take in order to limit risks and guarantee security to their citizens (Aradau and Van Munster, 2007). The first main consequence of the arising of these uncontrollable risks, especially terrorism, was that private insurance has become obsolete in the risk society, because of their inability, or unwillingness of bearing the huge amount of costs of unpredictable catastrophes, such as terroristic incidents (Aradau and Van Munster, 2007). Therefore, because private insurance was no longer able to cover all the new types of risks arising, a state action was required in order to maintain order and security in the society, particularly after the event of September 11th. The second principal change was the emergence of a new type of risk, precautionary risk, applied to what is uncertain in order to give at least a general line of how presumable incalculable catastrophic risk such as terrorism could be governed (Aradau and Van Munster, 2007). Taking precautions against terrorism and other not easily calculable risks has become as relevant as insurance action for mitigate the costs of risk consequences. Precautionary risk is based on the analysis of the worst-case scenario and on achieving the scope of having zero risk; they both are two interrelated ways which may improve the governability of the risk society. A new concept arises from the precautionary risk: no level of risk is acceptable, it has to be avoided at all costs. As a consequence, this innovative view has broken the equation that specify that a risk was acceptable as long as it is reparable or repaired (Aradau and Van Munster, 2007).

Precautionary risk management implies a very high level of surveillance of the population, which entails a more pro-active role of governments in extending surveillance measures for

avoiding every possible dangerous situation. In order to maintain security in the risk society, new measures and techniques of prevention were implemented and reinforced with the use of huge amount of sophisticate technologies such as biometric identifiers and biographical profiles, for allowing decisions to be taken with the highest possible horizon of certainty (Aradau and Van Munster, 2007).

To sum up, the new catastrophic risks analyzed by Beck (that are terrorism, environmental damage, and financial crises), have emerged from the macro-sociological transformation from the industrial society to the much more complex risk society (Beck, 2002). The uncertainty of risk occurrence and its disastrous effects has led to the introduction of new methodologies for threating risk, a dynamic phenomenon which is becoming more and more complex, difficult to prevent and interconnected with the society. New precautions actions are mandatory in order to protect the security and the wellbeing of human people from the major threat of terrorism (Aradau and Van Munster, 2007).

1.4.2 The concept of Terrorism risk: difficulties and changes in the hedging procedures.

In the previous sub-section, the analysis of the relationship between terrorism and risk society has demonstrated the importance of finding a form of hedging against this complex and dynamic threat. The event of 9/11 has created a radical break with the past, accelerating risk management programs, improving prevention and mitigation actions (Amoore and De Goede, 2005). Consequently, Governments became aware of the drastically underestimation they have made on terrorism and the high exposition of their risk portfolio to terrorism risk consequences. Therefore, the conventional methods of insurability of terrorism risk were put into question, mainly because of their inability to hedge against such disastrous event like 9/11 (OECD, 2005). In fact, the highly level of correlation between risks and the growing unpredictability of them, have made modern terrorism risk as one of the most difficult to predict and challenging risk for insurer institutions. The main reason is connected to the specific features of terrorism risk, that are quite unpredictable and dynamic. They can be divided in five different factors that together made terrorism risk very different from the other types of extreme events (OECD, 2005):

1) Limited importance of historical data: the analysis of past intentions of terrorists is not particularly relevant for future predictions. Available data from past events does not reveal enough information about the future patterns of terrorist attacks. In addition, terrorism is a very dynamic risk, therefore it is possible the continuous arise

of new terrorism's forms in a close future that made the previous researches almost useless. The crucial difference between terrorists' modus operandi before and after September 11th is the main example;

2) Dynamic nature of terrorism: it is able to adapt to prevention strategies adopted by governmental authorities, by shifting terrorists' attention to other unprotected targets in order to maximize the success of their attacks;
3) Interdependent security: it is a possible negative externality that may influence the decision-making process of terrorism prevention plans. An insurer may suffer losses if it has activities connected with other economic actors that fail to implement the right prevention actions;
4) Unavailability of information: it can affect both the insurer and the insured, principally because Government do not usually disclose information about terroristic activities and future possible targets for national security reasons. The only information available is the ones contained in historical database, but it is not sufficient for making a correct prediction of terroristic activities;
5) Government influence on the risk: it influences the risk predictability through their foreign and domestic policies, as well as counterterrorism plans, by changing the terrorists' choice of target (OECD, 2005).

All these challenges create a consistent risk ambiguity which make terrorism arduous to hedge compared to other disaster event.

In addition to the previous factors analyzed, all the four insurability criteria are not exactly matched by terrorism risk (OECD, 2005). Assess ability, which is the possibility to quantify severity of losses and probability of occurrence, is not met because of the unpredictability and impossibility to predict the severity of a terroristic attack. Randomness, which is the specific time at which the event may occur, is also not met because terroristic attacks happen randomly without a specific pattern and the third criterion, economic insurability, that is the possibility to calculate an accurate insurance premium commensurate with risk, still remains very difficult to match with terrorism risk because of the impossibility to predict the severity of a terroristic attack. Finally, the last criterion, mutuality, which is the possibility to create a risk community with the persons exposed to terrorism with the aim of sharing this risk, is the only one that can be met in more convenient way. For all these reasons, terrorism risk constitutes a critical challenge for the insurance industry, and it can explain the inability to prevent the incident of the Twin Towers of 2001 (OECD, 2005).

After the analysis of all the difficulties in predicting terrorism risk, governmental authorities, in collaboration with global agencies, have implemented several changes in order to improve their responsiveness to the threat of terrorism (Amoore, De Goede, 2005). The first possible answer for improving their ability to predict terroristic actions was the increasing reliance on new and more sophisticated technologies and computerized data-mining (Amoore, De Goede, 2005). Secondly, the private insurance was replaced by state intervention and insurance[17] that has led to further improvement in hedging terrorism risk, especially because of the great majority of information that the state possesses compared to the ones owned by privates. Finally, experts' opinions were replaced by states and intelligences agencies much more informed and efficient that the formers (Beck, 2002).

A new and more effective quantitative terrorism risk assessment was developed with the aim of classifying all the possible terrorist risk scenarios. The multitude of scenarios is basically related to the fact that terrorism has several forms and attack's typologies and so very different possible outcomes (Woo, 2002). For that, the scenario analysis conducted for terroristic events is different and more complex that natural perils (storms, earthquakes and floods). In this case, the human dimension to conflict must be incorporated, because terrorism is a voluntarily action made by living people with the only scope to hurt other human beings (Woo, 2002). Therefore, considering a sociologist approach, it must be taken into consideration human factors as intelligence, network of relationships of the terroristic organization, social interactions among terrorists and between terrorists and people, and at the end, the hierarchical structure of terroristic groups. For improving the quantitative terrorism risk assessment, risk managers must consider the terrorists' adapting capability of learning from past experiences, either failures or success, and to use their collective intelligence for understanding the fundamental characteristics of social organization spread into the population (Woo, 2002).

The structure of the terroristic organization is the first element to consider in order to preventing possible terroristic attacks (Woo, 2002). In fact, the effectiveness of terroristic actions mainly depends on the features of the group, also considering that terrorists can only hope to achieve their goals through efficiency and adaptability of the maneuver, because they are always outnumbered in terms of weaponry and combat capability (Woo, 2002). Centralization and hierarchy clearly influence the terroristic organization ability to resist to

[17] The principal state intervention was the implementation of the Terrorism Risk Insurance Act also called TRIA. It is accurately explained in chapter two as it is one of the main topics of the thesis

counterterrorist intervention: the less hierarchical and centralized, the more resilient the organization is. One of the most common architecture for a terroristic group is the one that involves multiple independent hubs, that serves as control center for the numerous satellite cells. To maximize their survival chance, they are dispersed over different nations and even continent, and this made very difficult the identification of these hubs, the activity of collecting information and therefore the risk management techniques for covering terrorism risk (Woo, 2002). These wide varieties of analysis are the basis used for preparing reliable models[18] for the efficient estimation of terrorism risk (Woo, 2002).

Finally, capital market plays a relevant role in terrorism risk coverage as a substitution of deficient insurance policies (Bouriaux and Scott, 2004). For this purpose, catastrophic bonds were created, also called CAT bonds. They are high-yield debt instruments that are insurance-linked and raise money in case of catastrophic events, natural or man-made. Several studies have demonstrated that the allocation of a small portion of investors' assets in this type of bonds creates more efficient portfolios[19] (Bouriaux and Scott, 2004).

To sum up, despite all the difficulties in applying hedging procedures, several changes have been made to better manage and prevent terrorism risk and its consequences, considered as one of the major threats that is now afflicting the global risk society. Because of its dynamic and unpredictable nature, terrorism is a phenomenon that must be faced by Governments in collaboration with global entities, through the application of new approaches that enable to forecast possible future terrorism risk's developments and promptly stop them (Bouriaux and Scott, 2004).

1.5 Conclusion

Through the analysis elaborated in chapter one, several issues and results were deduced by the context. The first issue of the investigation is the complicated definition of terrorism, a phenomenon that is still today not perfectly understood and very difficult to prevent. Giving a univocal definition of terrorism is a great advantage for achieving a more functional international collaboration between countries in order to have a faster response to terroristic attacks (Mahmood, 2002). Without this definition it is impossible to prepare lines of responsibilities that can be charged against states that support terrorism (Mannik, 2009 and

[18] The models applied for estimating terrorism risk are explained more in depth in chapter two section four.

[19] Capital markets solutions in order to hedge terrorism risk is treated and explained in chapter two section three.

Mahmood, 2002). In addition, strategies and reasons behind the major terroristic attacks are continuously changing, because of terrorism's dynamic nature and their complex organizational structure, especially created for avoiding counterterrorism actions (Woo, 2002). Therefore, terrorism risk insurability results in a consistent problem for insurer, principally because it doesn't match the insurability criteria and because of its specific characteristics (OECD, 2005). It is particularly unpredictable in terms of severity of losses and probability of occurrence and moreover, historical data are almost useless for its prediction. All these aspects have made terrorism risk one of the main issues in the contemporary risk society (Amoore and De Goede, 2005). The reactions to this threat have been particularly reinforced during the decades after the terroristic attack of September 11th, which has resulted in a turning point in the history of counterterrorism (Beck, 2002). The result to that disastrous event was a great improvement in the responsiveness tactics against terrorism. New and more sophisticated technologies were implemented, and countries in collaboration with global agencies have put more reliance on them than on experts' opinions (Amoore, De Goede, 2005). In fact, because emerging prevention strategies must adapt to the mutable conditions and environments in which terrorism is active, state intervention was absolutely required, principally because states possess much more information than private sectors (Beck, 2002). The last result concerns the substitution of private insurance measures with new public insurability techniques in order to improve the precise hedging techniques expressly created with the scope of prevent and mitigate terrorism risk consequences (Beck, 2002).

CHAPTER 2. Models and Insurance Policies for Measuring and Hedging against Terrorism Risk.

2.1 Introduction

Chapter two presents an extended analysis of conventional and unconventional methods for hedging against terrorism risk and also explains the importance of modelling terrorism risk (Vickers, 2015, OECD, 2005 and Willis, Al-Shahery, 2014).

This chapter is basically divided into four sections which explain four different concepts. The first section, after a brief analysis of the main difficulties in hedging techniques against terrorism risk, carefully describes the most important terroristic insurance and reinsurance policies applied by OECD countries for counter-terrorism actions (Michel-Kerjan, 2012). The section specifically examines the functioning of Terrorism Risk Insurance Act (TRIA), an insurance program implements by the U.S. in the aftermath of September 11th (Risk Management Solutions Report, 2012), and it defines the role of Governments in providing assistance to private insurance markets, its forms of intervention and limits (Kunreuther, Michel-Kerjan, 2007). Section two instead, explains the alternative methods implemented by capital markets for providing an effective coverage against terrorism risk. Basically, these solutions are used to overcome the limits of conventional insurance and reinsurance policies, and they are divided into two main groups: alternative risk financing instruments and alternative risk transfer tools (OECD, 2005). This section also provides an accurate explanation of terrorism bonds and captive insurance, two of the most important unconventional tools used by capital markets (Bruggeman, 2007). The following section, underlines the usefulness of terrorism risk models which furnish a continuous flow of information in order to prevent and mitigate the effects of terrorists' attacks (Willis, Al-Shahery, 2014). Section three presents three different models (Attacker-Defender model, three variables terroristic model and social network analysis model), each with its own specific characteristics and limits (Major, 2002). Finally, section four aims at explaining and describing the main benefits related to the implementation of hedging techniques against terrorism risk. To achieve this goal, the section presents also a cost-benefit analysis about covering policies to demonstrate that the advantages far outweigh the drawbacks (Gold, 2004).

2.2 Insurability of Terrorism Risk

The section briefly explains the difficulties in hedging against terrorism risk and it describes the most relevant terroristic insurance and reinsurance policies applied by developed countries for counter-terrorism actions. It is divided in two sub-sections: the first one gives an accurate analysis of principal terroristic insurance policies by focusing the analysis on the Terrorism Risk Insurance Act (TRIA), which was implemented by the U.S.A after the terroristic attack of September 11th in 2002. Sub-section two defines the role of Governments in fighting this threat, accurately explaining their forms of intervention (ex-ante, ex-post, direct and indirect) and their limits and drawbacks.

2.2.1 Principal Insurance Policies against Terrorism Risk: focus on TRIA.

During the aftermath of the terroristic attack of September 11th, insurance industry and Governments have faced a significant change in the treatment of terrorism risk, due to the several difficulties encountered in containing this emerging threat (Vickers, 2015). Terrorism risk is a triple challenge for the insurer: a conceptual challenge because of the problematic identification and analysis of it[20], a technical challenge linked to the difficulties in terrorism risk quantification and assessment, and an operational challenge due to the expensive operation in terms of time and costs for monitoring and for implementing risk management techniques in order to control this dynamic phenomenon (Vickers, 2015). Terrorism risk has to be correctly understood at both macroeconomic and microeconomic level in order to recognize its true costs and therefore the correct intervention for minimizing these costs (Vickers, 2015). Governments and insures have recognized two terrorism costs: direct costs that impact immediately the economy through damages to property, business and people, and indirect costs, which possess a huge impact in the years coming, radically changing people mindset and economic trend (Kunreuther, Michel-Kerjan, 2007). Hence, in the immediate period after the terroristic attack of September 11th, 2001, global insurers, and especially the ones working in the U.S., have found themselves with a very high amount of terrorism risk exposure not hedged in their portfolios and with very limited possibilities of reinsurance in order to reduce and prevent probable future losses due to other terroristic attacks (Kunreuther, Michel-Kerjan, 2007). By the early 2002, 45 nations have permitted

[20]In chapter one there is the explanation of the difficulties encountered in giving a unique definition of terrorism. Without a common definition, it is difficult to understand which actions are terrorism-related.

insurance companies to exclude terrorism coverage from insurance policies with the exception of workers' compensation. In addition, because of the numerous obstacles for insurers in creating valid terrorism risk insurances and for their high costs, the need for governmental intervention became essential (Kunreuther, Michel-Kerjan, 2007). Insurance industry could not support alone the threat of terrorism especially because of its complex nature that challenges its correct insurability. In fact, it is particularly unpredictable and dynamic, with limited or not historical data available and with few information that can be useful[21]. Finally, it affects the economy in several ways: terrorism damages human and physical capital, it increases the level of uncertainty and it negatively affects specific industries such as the airline, tourism and insurance sector (Vickers, 2015).

Therefore, political pressure forced Governments to act and implement anti-terroristic actions and gives them the duty to identity, analyze, measure and treat terrorism risk in order to protect the safeguard people well-being (Vickers, 2015). The first way implemented by Governments for covering terrorism risk is through proactive measures. This means preparing policy measures for mitigation, preparedness, response and for improving the recovery capacity of a community after terroristic hazards (Vickers, 2015). Each OECD[22] country has developed its personal and particular solution in order to mitigate terrorism threat, considering their past experiences, their technologies and especially the types of terroristic groups active in their territory. The OECD countries that have more suffered from terrorist attacks on their soil are Israel, Spain, France, the U.K. and Germany, without considering the U.S., that have applied the most famous and important insurance program (TRIA) which will be accurately analyzed in the next pages of the chapter (Michel-Kerjan, 2012). Four out of the five mentioned countries have developed terrorism insurance that is supported by government guarantees, while Israel has used a different approach (United States Government Accountability Office, 2005).

1) Israel has developed an insurance policy based on governmental coverage without the involvement of private insurers. Because of their long history of terroristic attacks, all losses from this hazard are fully compensated by the state. Therefore, any kind of direct and indirect damage linked to terrorism is hedged by a public

[21]In chapter one section three all terrorism specific features are explained (OECD, 2005).

[22]The acronym OECD stands for Organization for Economic Co-operation and Development. It is an intergovernmental organization which includes the most developed countries in the world and it was founded in 1961.

compensation fund regulated in 1961. The fund is made by a general property tax collected across the entire nation according to Israel regulations. There are specific individual and business compensation which are furnished to people who have suffered from terroristic attacks (Michel-Kerjan, 2012);

2) In Spain, terrorism is covered because it is considered part of the government insurance compensation scheme for disaster risks called "Consortio de Compensation de Seguros", created in 1954 and reorganized after the terroristic attack in Madrid in 2004. Terrorism risk is included as an optional cost to property insurance sold by private insurers, who are not responsible for losses. Basically, commercial firms pay 0,21 euros per thousand of property coverage and in addition 0,25 euros for possible business interruption in order to benefit from the state insurance against disaster risks such as terrorism (Michel-Kerjan, 2012);
3) French government has implemented in 2001 a public-private partnership called GAREAT that works as a co-reinsurance pool organized with a tier structure. The state layer (the third and final level of the structure) is an unlimited guarantee by the French government that uses the "Caisse Central de Reassurance" as a state-owned reinsurance company. In France, terrorism risk insurance is compulsory, and it covers several types of risks that can cause business interruption, including chemical, biological, radiological and nuclear attacks (Michel-Kerjan, 2012);
4) In the United Kingdom, after the terroristic event of April 1992 when a bomb explosion in London costs almost 700 million dollars to insurers, it was created a mutual reinsurance organization called Pool Re, with the specific aim of guarantee claims consequences of terroristic attacks on commercial and industrial properties in order to compensate business interruptions and property damages. Pool Re act was extended to all type of risks and it acts as a reinsurer for all the insurers which want to be a member of the organization. It basically shares ten per cent of its collected premium with the United Kingdom government that provides this complete coverage (United States Government Accountability Office, 2005);
5) In Germany, before the events of 9/11, the terrorism coverage was part of all insurer policies but there was no extra premium to be paid. After September 11th, the very limited terrorism coverage has led to the creation of the federal government-backed property insurance corporation Extremus AG. It is not a reinsurance institution, but it acts as private insurance company. It's annual coverage capacity in case of hazards is around ten billion euros divided in two layers (national and international insurance

and reinsurance companies for the first two billion and federal government for the rest) providing coverage for building, contents, and business interruption. Finally, it is not mandatory as in the U.K. (Michel-Kerjan, 2012).

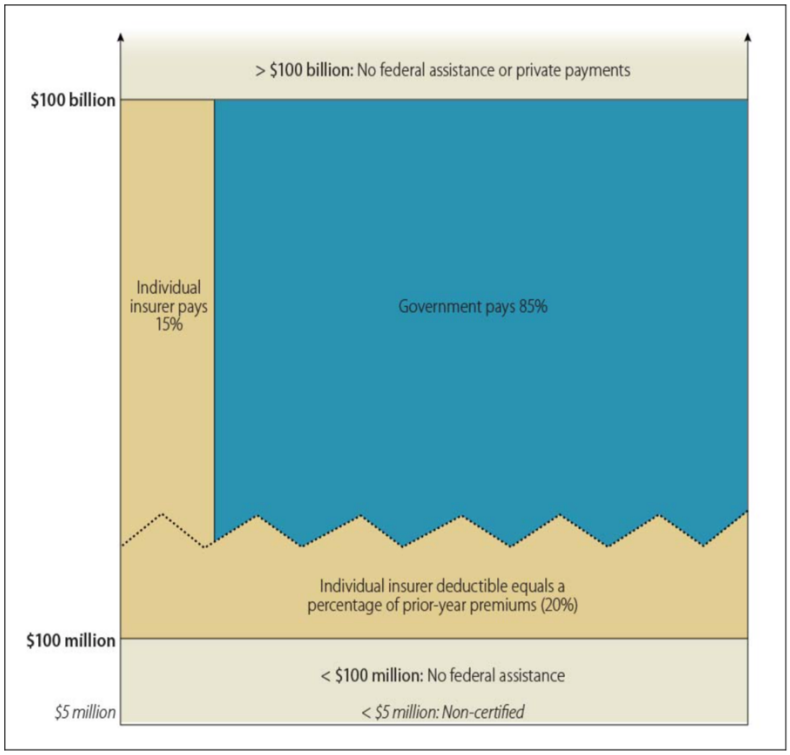
The most important Government intervention in order to control and mitigate terrorism risk was the insurance program developed by the U.S. in 2002 (Webel, 2013). In this nation, prior to the disastrous event of September 11th, insurers generally did not explicitly hedge against terrorism risk, but in the aftermath on 9/11 they understood the magnitude of this incoming and dynamic threat (Webel, 2013). The insurance market was unprepared to a similar catastrophe and in few months terrorism risk insurance became unavailable or extremely expensive because a large number of state regulators decided, concerned about the pressing insurers request, to exclude terrorism risks from commercial policies (Willis, Al-Shahery, 2014). Therefore, several businesses where not able to purchase insurance policies against terrorism risk and so, they remained unprotected to eventual future terrorism hazards (Webel, 2013). Governments were especially concerned about the impossibility to protect and ensure specific economic sectors such as transportation, construction, energy and utility services that can be targets for future attacks (Webel, 2013).

In order to respond to the fear of economic damage due to the absence of commercially available coverage, in November 2002, the U.S.A Congress intervened by enacting the Terrorism Risk Insurance Act (TRIA), that provided a federal backstop for insurance claims linked to terrorism activities, created as a provisional measure until the insurance industry has developed an adequate solution for hedging against terrorism risk (Risk Management Solutions Report, 2012). According to the pre-mentioned TRIA, Governments would provide partial coverage for damages created by terrorism activities. The implementation of TRIA in the U.S. has ensured the quick availability and affordability of terrorism coverage for commercial and industrial businesses and it has helped the recovery in the aftermath of September 11th. It was also a measure that inspired a large number of OECD countries to establish a public-private terrorism pools in order to cover all the losses in case of eventual terroristic attacks (Risk Management Solutions Report, 2012). Simultaneously to the implementation of TRIA, insurers understood the importance of improving the quality and resolution of their data in order to have better estimates on terrorism risk exposure in their portfolios. They moved to an innovative risk-based approach that was based on new technologies not available before 9/11 such as geographic information system (GIS) and

aerial imagery for visualizing potential terrorist targets and assess the relative risks (Risk Management Solutions Report, 2012).

The Terrorism Risk Insurance Act had three main goals: to create a provisional federal program base on a private-public partnership in order to compensate the insured for terrorism losses and to stabilize the insurance market, to protect customers providing available insurance policies against terrorism risk, and finally, to preserve the state regulation of insurance (Kunreuther, Michel-Kerjan, 2017 and Webel, 2013). According to that act, government intervention was related to the size of the insured loss: for relatively small losses under 100 million dollars there was no federal sharing; for medium sized losses, government role was to spread the loss over the entire insurance industry and providing assistance up front; for large losses the federal government has to pay the largest part of them and in case of more than 100 billion dollars loss, there is no federal government coverage and no requirements that private insurers will provide hedging (Kunreuther, Michel-Kerjan, 2017 and Webel, 2013).

Figure 4. Initial loss sharing under TRIA program of 2002.



Source: Webel B. (2013), "Terrorism Risk Insurance: Issue Analysis and Overview of Current Program", Congressional research service, pp. 1-15.

Figure four illustrates the different thresholds of losses in million and billions of dollars explicitly specifying the levels of federal government intervention in case of terroristic damages. It also underlines the percentages of government and individual insurer payments in case of large losses (between 100 million and 100 billion of dollars), respectively 85% and 15% (Webel, 2013). With the introduction of TRIA, the premiums of terrorism insurances where substantially reduced and stabilized compared to the previous level and by providing financial protection to anyone who suffer from losses from terroristic attacks, either citizens of the country or foreigners, the insurance program has drastically improved its equitability (Kunreuther, Michel-Kerjan, 2007).

During the following decade after the TRIA authorization in 2002, the continuous request for governmental coverage on terrorism risk, has led to a twice extension of the program through the U.S. Congress amendments, who legislated the Terrorism Risk Insurance Program Reauthorization Act (TRIPRA) in 2007 which had to terminate in December 31, 2014 but it was successively re-extended until 2020 (Marsh & McLennan Companies Report, 2015). These two extensions, especially with the introduction of the TRIPRA, have made several changes to the previous program, mainly concerning the covered acts, passing from covering only the foreign terrorism in the U.S. and on U.S. interests abroad to the coverage of both foreign and domestic terrorism in the U.S and on U.S interest abroad, and the change in the percentage of federal reinsurance quota in case of terrorism damages from 90% between 2002-2005 to 85% from 2007 (Marsh & McLennan Companies Report, 2015)[23].

2.2.2 The Role of Government in hedging against Terrorism Risk.

In the last decades, terrorists have increased their activities and improved their capabilities in order to impose their authority over the population and to defeat eventual counter-terrorism actions made by national governments for mitigating terroristic attacks and damages on properties and human well-being (Kunreuther, Michel-Kerjan, 2007). The need for government intervention was absolutely necessary in order to overwhelm this threat. Federal insurance programs appeared to be the best possible solution especially because

[23]More information about the several secondary changes happened with the introduction of the TRIPRA are accurately illustrated by Marsh & McLennan Companies Report (2015), "Terrorism Risk Insurance Program Reauthorization Act".

governments are the only one able to cover enormous damages such as the ones created by terroristic incidents of September 11th, moreover they possess better and restricted information about terrorist's activities and, with their intervention, it is possible to decrease the level of uncertainties that sharply increased after 9/11 (Kunreuther, Michel-Kerjan, 2007). National government play a crucial role in the phase of prevention and management of terrorism risks. They have established and implemented strong and comprehensive counter terrorism policies with unique scope of limiting the future occurrence of terrorist attacks (OECD, 2005). On the contrary, private market solution, which is the option that let the market operate in complete independence in hedging against terrorism risk, was not anymore a solution without at least a partial government intervention (OECD, 2005). Therefore, governments and insurers must work together in order to assess risks and define the correct risk management approaches and at the same time improving the use of available resources in most effective way for minimizing the terrorism risk exposure (Vickers, 2015).

For the insurance sector, there are three essential approaches to public policy, and in addition, there isn't an optimal approach because they are strictly dependent on several variables such as changing legislation, presence of market failures, risk management techniques, type of terroristic groups active in the country and so on (Vickers, 2015) ... The three ways are:

1) Laissez-fare policy, that underlines the market-base equilibrium able to provide the most efficient allocation of resources and hence the most effective way and insurance policy for covering terrorism risk, even with limited government intervention;
2) Public interest theory, which is the opposite of the first one, and therefore suggests that only governments can provide a solution to this problem because the market is afflicted by market failures[24] and it cannot provide a solution for itself;
3) Market-enhancing view, which takes a position between the two approaches, considering the importance of public policies that should facilitates the development of the private insurance industry, by providing a constant flow of information. This theory does not expect the creation of federal institutions in substitution of private ones (Vickers, 2015).

[24] Inequality and asymmetric information are the two most relevant market failures related to terrorism risk. They can be partially eliminated by government intervention (Vickers, 2015).

In the last two approaches, where government intervention is present, there are two different categories of actions that can be implemented by governments in order to provide assistance to the insurer industry (Rhee, 2005). The first one divides government intervention in "ex post" actions or also called ex post government subsidy, while the second group is made by the "ex ante" government solutions (Rhee, 2005). The ex post government actions are mainly concerned on providing subsidies to victims of disasters, terrorism attacks or great tragedies. In the aftermath of 9/11 the U.S. government has responded with a huge number of subsidies for permitting the simultaneously quick recovery of people wellness and United States' economics. It was created the September 11th Victim Compensation Fund with the double scope of limiting the liabilities of the airline industry and providing a generous compensation for the victims of the terrible incidents, who may have not previously subscribed a life insurance (Rhee, 2005). Other possible actions for large businesses that may not receive direct government welfare are special tax benefits or low interest loans in order to stimulate the economic recovery and also indirectly compensate the losses (OECD, 2005). In summary, ex post actions are motivated by the idea of enforcing measures for promoting stability and equitability (Rhee, 2005).

The second group of actions are the ex-ante government intervention which are specific government sponsored risk pool approaches with the aim of allowing the rapid and efficient allocation of the resources destined to the compensation of terrorism-related losses (OECD, 2005). A large number of nations have taken advantage from these public-private partnership, especially because government programs are able to increase the overall resources and capacity to control terrorism risk and moreover they can spread risks to deeper pockets. Only with the assistance of federal government, there is enough capital to absorb multiple shocks from terroristic attacks (Rhee, 2005).

The second category of government intervention is divided in indirect or implicit solutions and direct or explicit solutions (OECD, 2005). The first group is characterized by the adoption of policies with the scope of furnishing particular incentives in order to restart private insurance and non-insurance markets. The most common forms of intervention can be fiscal and regulatory measures for facilitating the raising and reserving of capital by insurance enterprises which were involved in terrorism disasters, or fiscal and regulatory incentives to facilitate the purchase of terrorism risk coverage. Another possible measure shall be the development of alternative risk transfer tools aimed at spreading the risks on

capital markets[25] (OECD, 2005). On the contrary, direct or explicit forms of government intervention were created in order to increase terrorism insurance availability and affordability, and they are evaluated as a complement to indirect forms of intervention being part of an integrated terrorism risk management plan. This type of measures can assume different forms with different scopes:

1) Government as primary insurer with the aim of providing directly insurance coverage to all policyholders. It is the most equitable and comprehensive, but also the most invasive measure;
2) Government as reinsurer of last resort that furnishes a backstop to private insurance exposures;
3) Government as lender of last resort which provides a higher availability of liquidity to the insurance and reinsurance industries after the occurrence of terrorism-related losses (OECD, 2005).

Giving all the possible forms of government intervention it is also important to underline the possible limits and drawbacks related to these measures (OECD, 2005). One of these limits is the probability of having potential operational rigidities and bureaucratic excesses in the operations of national compensation scheme. Another possible drawback is the high probability that government intervention crowds out or displaces private markets, especially if it is acting as primary insurer, considerably limiting private insurance industry maneuver. The last drawback happens when government intervention substantially reduces the incentives to propose private mitigation actions. It usually happens because government intervention can temporarily manage terrorism risk and therefore private insurance industry relies on public sector strategy without creating future possible precautionary measures for avoiding other disasters (OECD, 2005).

2.3 Alternative capital market solutions for containing Terrorism Risk

This section mainly explains the several alternatives considered and implemented by capital markets in order to mitigate, control and prevent terrorism risk. It is divided in two sub-sections in which firstly, they are briefly illustrated all the capital market solutions that can be used to overcome the limits of conventional insurance and reinsurance markets, and

[25] This argument will be better explained in section three which illustrates the possible financial market solutions and alternatives in order to contain terrorism risk.

secondly, it accurately explains the first category of alternative risk management solutions, which are the unconventional risk financing methods, with a specific focus on captive insurance. Sub-section two instead, explains the second category of capital market solutions called alternative risk transfer measures, and there is a deeper analysis on catastrophe bonds that permit the origination of terrorism bonds.

2.3.1 Alternative risk financing solutions for hedging against Terrorism Risk.

Conventional insurance and reinsurance markets, very often stabilized and regulated by government interventions as previously analyzed in section one, are not the only possible solutions in the practice of hedging against terrorism risk (OECD, 2005). Capital markets may offer several different types of alternative risk management solution for covering terrorism risk that can be basically divided into two groups: unconventional (or alternative) risk financing instruments and alternative risk transfer methods[26]. The markets that contains these risk financing and transfer solutions offer a vast range of contingent capital instruments, risk-linked securities, risk swaps and catastrophe derivatives (OECD, 2005). There is a basic difference between the two pre-mentioned categories: alternative risk financing instruments have the specific scope of offering high availability of funding in order to accelerate the economic and social recovery of a community who has suffered from terrorism losses. The second group, unconventional risk transfer instruments, aim at shifting all or part of the financial weight associated with terrorism risk to one party to another (OECD, 2005). It is the reason why these risk transfer instruments are considered the principal alternative to conventional insurance contracts. Anyway, the former and the latter tools can be jointly used with the aim of creating a common framework for terrorism risk management strategy (OECD, 2005).

The purpose of alternative risk financing tools is to guarantee access to future financing opportunities under predetermined conditions. There are different forms of risk financing solutions which have been created by international financial markets to secure protection against eventual terroristic events (OECD, 2005). The most important ones are the committer funding arrangements with commercial banks, like committed revolving term facilities and contingent capital tools which are offered by banks and securities firms. The second instrument has the scope of issuing medium-term securities on fixed terms if a certain trigger

[26]This group is just mentioned in this brief introduction and it will be analyzed in the second sub-section.

event arises. Anyway, until today this kind of instruments has a very limited use on terrorism risk coverage, in fact no contingent capital instruments has been issued using terrorism attacks as triggering events (OECD, 2005).

Another instrument that can be used as alternative risk financing measure is the captive insurance. Even if it is usually think as a risk transfer vehicle, it can be used as a risk financing tool by enterprises when the insurance market is not able to furnish enough flexibility, stability and attractive conditions of coverage (OECD, 2005). A captive insurance firm is considered as an insurance enterprise that is 100% owned and managed by its insureds with the particular purpose of ensuring the risks of its owners, and therefore the principal beneficiary of its underwriting earnings is the insured (Riley, 2016). Basically, captive insurance offers a better and broader coverage than normal commercial insurance policies, and at the same time, organization may obtain a significant cost improvement in managing their terrorism risk (Marsh & McLennan Companies Report, 2018). It can happen that captive owners pay the same cost both for implementing a terrorism insurance program and for buying it from commercial insurers (Marsh & McLennan Companies Report, 2018). There is a vast range of captive insurance companies, such as pure captives, industrial insured group captive, association captives and sponsored captives, where the most common form is the single parent pure captive (Riley, 2016). Therefore, many nations have recognized the utility of this form of insurance and the need for creating specific regulations in order to better managed the implementation of captive insurance. In the U.S., with the introduction of the Terrorism Risk Insurance Act, the Vermont Captive Insurance Association (VCIA) has convinced the Congress to establish a regulation in order to control the mechanism of captives (Riley, 2016). At the end of the debate between the two parties in 2003, where the VCIA requested a non-mandatory participation in TRIA program for captive insurers, especially because they usually operate outside the traditional insurance market, and so they should not be considered as normal insurance firms, the Congress declared that all captive insures has to be integrate in the new terrorism insurance program (Riley, 2016). Despite that decision and the importance in the risk management strategies in global business and especially in the U.S. economy, the application of TRIA to captives has given uncertain results and also their role in the pre-mentioned program is ambiguous and not particularly relevant (Riley, 2016).

In summary, it has to be underlined that especially regarding terrorism-related losses, captive insurance seams to not offer adapted solutions to the current constraints which normally

affect the availability of reinsurance coverage requested for terrorism risk exposure (OECD, 2005). This is the main reason why usually the most common unconventional capital markets instruments implemented for hedging against terrorism risk are part of the alternative risk transfer category (OECD, 2005).

2.3.2 Alternative risk transfer expedients in the coverage of Terrorism Risk.

As previously said, alternative risk transfer instruments are special tools used by capital markets in order to shift all or at least a part of the financial weight associated with terrorism risk to one party to another, and moreover they are considered the most efficient alternative to conventional insurance and reinsurance markets for hedging against terrorism risk (OECD, 2005). At the beginning, insurance companies have created these alternative transfer instruments for having protection against natural catastrophes such as hurricanes, windstorms, floods and earthquakes, and their first issuance on the capital market happened in 1994, which has led to the creation of the catastrophe bond[27], the first capital market instruments linked to disasters risk (Vickers, 2015). Therefore, it is clear that alternative risk transfer instruments are a special product or solutions that transfer risk exposures from the insurance market to the capital market in order to achieve risk management goals. It appears to be used both for mitigating the effects of hard market and for better managing complex risk exposure positions that cannot be insured by the traditional insurance market (Bruggeman, 2007). The alternative risk transfer market is divided in two categories: risk carriers and solutions. The first group mainly contains three types of alternative risk carries:

1) Self-insurance and captives[28];
2) Risk retention groups;
3) Capital markets instruments.

On the other hand, the second group considers a large number of possible solutions that can be implemented instead of conventional insurance, starting from finite risk insurance tools, contingent capital, multi-trigger products, securitization and insurance linked securities,

[27] In this chapter the analysis is mainly focus on catastrophe bonds because they were particularly relevant in the creation of terrorism bonds, with whom share similar characteristics.

[28] Captive insurance has a double possible use as alternative risk financing instruments and unconventional risk transfer tool as previously analyzed in sub-section one.

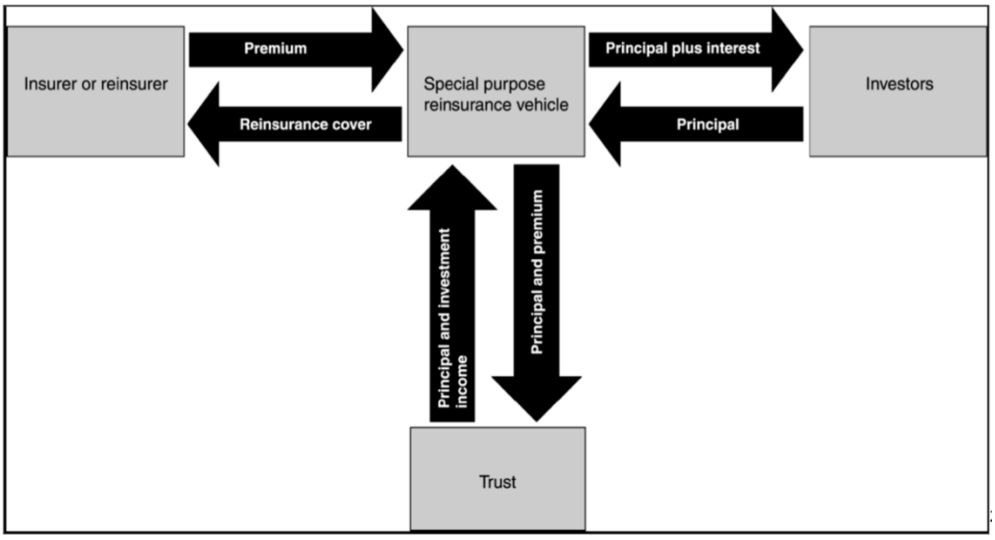
until special catastrophe derivatives (Bruggeman, 2007). All these alternative risk transfer tools possess common characteristics that can be used in order to identify the tools:

1) Tailor made solutions;
2) Multi-dimensional coverage, which means several years of coverage and multi-line coverage;
3) For facilitating the insurance of uninsurable risks, they provide tools for risk transferring;
4) Incorporation of financing tools, like derivative instruments;
5) The use of a large component of finance.

All these alternative solutions were principally created because of several factors that has affected their growth, such as the high volatility of traditional insurance markets, the high cost of traditional reinsurance policies, the inability to cover natural or man-made disasters with the traditional insurance and reinsurance measures, and finally, the need for improving the efficiency of capital usage and risk diversification (Bruggeman, 2007).

All these measures have been usefully applied for covering natural disasters, but even if capital markets solutions and especially alternative risk transfer instruments are a good candidate for undertaking terrorism risk hedging, only catastrophe bonds seems to be really effective compared to all the other analyzed measures. Moreover, terrorism risk coverage is a longer tail business than natural catastrophe coverage, and therefore this makes terrorism risk even harder to securitize that natural disaster risk (Bruggeman, 2007). Therefore, this innovative capital market instruments, terrorism bond, takes its origins from the previously quoted catastrophe bond, or also called cat bond. It has principally arisen because of the inability of the catastrophe reinsurance market to offer effective measures of coverage against disastrous events (Vickers, 2015). Catastrophe bonds are basically structured as Insured-linked Securities (ILS), but with exception that in case of a pre-specified disastrous event that occurs prior to the maturity of the bond, the investor loses the accrued interest and/or the principal value of the bond (Bruggeman, 2007).

Figure 5. The structure of a catastrophe bond /terrorism bond.



Source: Bruggeman V. (2007), "Capital Market Instruments for Catastrophe Risk Financing", American Risk and Insurance Association, pp. 1-40.

Figure five illustrates the structure of a catastrophe bond that is exactly the same of a terrorism bond with the only exception that in the latter the trigger event has to be brought back to a man-made disaster, such as a terroristic attack. A catastrophe bond offering is given by the use of a special purpose reinsurer (SPR), as illustrated in the image, which is an issuance vehicle that can be a normal insurance or reinsurance company (Bruggeman, 2007). This SPR has the scope to furnish reinsurance to a sponsoring insurance company and then sells it into specific notes to investors, and at the same time it has to provide and indemnity contract to the issuing company. The earnings made through the reinvestment and the premium payment from the issuing company generate the investor coupon. Therefore, the invested proceeds held in trust account are the principal way of repayment at maturity (Bruggeman, 2007). This kind of bonds usually pay a relatively high interest rate compared to other kind of capital markets instruments, and this means that the investor's reward for taking natural and man-mad disaster risk is high. Anyway, since the issuing company is exposed to possible future losses on its underlying catastrophe risk, but it won't have to provide payments to investors, it has effectively hedge its risk through the use of capital market tools (Bruggeman, 2007). Terrorism-related bonds, that share the same structure already explained, where introduced for the first time in the aftermath of the terroristic attack of September 11th. It was a successful idea especially because scholars have demonstrated that the allocation of a small percentage of investors' assets in catastrophe /terrorism bonds, creates a more efficient portfolio that can better mitigate the total risk exposure and provides higher rewards (Bouriaux, Scott, 2004).

On consequences, catastrophe and terrorism bonds possess their own specific advantages and drawbacks (Bruggeman, 2007):

1) They can be used as a complement to the vast range of basic risk management tools;
2) They permit the raise of more equity capital through the selling process of more company stock and the same time, they limit the risk exposure thanks to asset management and underwriting process;
3) They allow reinsurance companies to partially transfer their risk exposure to the capital markets rather than retain it;
4) Terrorism and cat bond have a small effect on reinsurance prices, avoiding their fast increase;
5) They possess really attractive risk/return characteristics, especially for large sophisticated investors such as hedge funds, and also, they have almost zero correlation with other currently traded assets and this means that are effective tools for portfolio enhancement and risk diversification purpose;
6) At the end they appear to be less volatile than normal stocks or bonds (Bruggeman, 2007).

However, it was also demonstrated that they possess very high costs compared with the costs of buying traditional reinsurance coverage. Firstly, they must face with higher interest costs that the insurer has to pay in order to provide compensation to investors that has bought a security which involve a substantial risk of losses. Secondly, there are very high transaction and administrative costs associated to this type of bond: transaction costs represent approximately the two per cent of the total coverage provided (Bruggeman, 2007). Moreover, there are several fees that have to be considered:

1) Underwriting fee charged by investment banks;
2) Specific fee charged by modelling firms for the development of terrorism risk models in order to predict severity and frequency of the hazards;
3) Fee charged by rating agencies for giving a rating to the security;
4) Legal fees for provisions and preparing disclosures for the investors.

However, catastrophe bond and terrorism bond can be cost competitive with the other more traditional reinsurance instruments appositely created for high-severity and low-probability risks.

To conclude, all these tools, both alternative risk financing and alternative risk transfer, seems to be useful in the practice of coverage of terrorism risk, by giving a valid

implementable option to the insurance market in addition to the conventional insurance and reinsurance policies. Anyway, in order to apply both conventional and unconventional tools, it is absolutely required the assistance of modelling firms that must develop reliable and efficient terrorism risk models for preventing and understanding frequency and severity of the events (Bruggeman, 2007).

2.4 Empirical models for estimating Terrorism Risk

Section four empathizes the importance of modelling terrorism risk in order to have more available and reliable information for preventing terroristic attacks. It is divided in four sub-sections: the first one specifies the importance of the activity of modelling terrorism risk, and moreover the basic structures of the models. Sub-section two gives a practical example of how terrorism risk can be control through the use of a game theory-based model. The third subparagraph describes terrorism risk as a function of three main variables: threat, vulnerability and consequences. The last one proposes an innovative model for measuring terrorism risk by using the social network analysis.

2.4.1 Introduction to Terrorism Risk models: usefulness and structures.

The complex and dynamic nature of terrorism risk and moreover, the limitations in using historical record to estimate its risk exposure, have put pressure on the insurance industry, scholars and governments to develop efficient model for measuring terrorism risk (Willis, Al-Shahery, 2014). The ultimate scope of these studies is to understand whether, when, where and how terrorists will eventually attack. In general, these models created by insurance industry combined physical modelling of attacks, some information about the geographic distributions of a country population, and expert judgments about the likelihood of attacks and their forms (Willis, Al-Shahery, 2014). Therefore, because of the almost infinite possibility of terrorists' attacks, target locations and types of actions, each of these developed models seems to be unable to measure and include all these variables, and therefore they cannot give a 100% accurate measure of terrorism risk. Anyway, these models have been continuously revised in order to give a better description of terrorism risk changes during decades, by using different assumptions for describing new terrorism intent and capabilities (Willis, Al-Shahery, 2014). They were useful for policymakers for understanding what vulnerabilities can threaten communities and infrastructures, and which

security measures and terrorism risk management strategy must be implemented in order to avoid future damages (Willis, Al-Shahery, 2014).

In the past decade, governments and insurance industry have faced relatively uncomplicated attacks, usually with conventional weapons, and so the activity of modelling terrorism risk was not particularly complicated especially because the frequency of these types of attacks remain constant and also the total level of losses won't be expected to exceed pre-specified amount that may be covered by the insurance industry's available capital (Willis, Al-Shahery, 2014). Unfortunately, with the terroristic attack of September 11th and moreover, because of the rapid development of new forms of terroristic attacks base on innovative weapons such as chemical, biological, radiological and nuclear weapons, the insurance industry has encountered several difficulties in measuring and successively covering this threat. Therefore, government intervention was absolutely necessary and was even more necessary the improvement of terrorism risk models, being the pivotal point in the analysis of terrorism risk and the most important instrument for developing adequate insurance and reinsurance policies on terrorism (Willis, Al-Shahery, 2014).

The improvement of terrorism risk models is also significant in the analysis of companies share prices changes (Karolyi, Martell, 2006). Scholars have demonstrated that democratic and developed countries experienced a large negative shock to their companies share price as a reaction after a terroristic incident. Moreover, the stock price reaction may reflect the possibility of future attacks, since the specific firm can be a target for one or more terroristic group. Therefore, it is fundamental the development of models that can measure this possibility in order to stabilize company's stock price alongside reinsurance policies (Karolyi, Martell, 2006).

In order to solve all these problems, terrorism risk modelling methods have been updated for several years since the two most important modelling companies AIR Worldwide and Risk Management Solutions have created and successively released the first terrorism risk models in 2002, in the aftermath of 9/11 (Marsh & McLennan Companies Report, 2018). They have focused attention on quantifying economic, property and human losses from terroristic attacks, and so, they have developed three different techniques to model terrorism risk:

1) Probabilistic models which estimate losses considering a large number of events. It is considered as a very uncertain approach, especially because the difficulties in predicting the probability of terrorism events;

2) Exposure concentration analysis that identifies and calculates the level of risk exposure around a specific potential target;
3) Deterministic models which are a compromise between the two pre-mentioned models. It is based on the analysis of a hypothetical scenario created considering potential damages on a specific target.

In addition to these new risk models, companies have created several new analytical tools for better measuring terrorism risk such as simulators of customized attacks to understand the expected impact to overall portfolios, or new risk mitigation strategies and so on… (Marsh & McLennan Companies Report, 2018).

In summary, it has been determinant the construction of innovative and more efficient techniques of risk modelling which allow the built of more functional business plans and the implementation of appropriate insurance and reinsurance policies for hedging against terrorism risk (Karolyi, Martell, 2006).

2.4.2 Game theory application to Terrorism Risk modelling: Attacker-Defender model.

In the aftermath of September 11th, the necessity for creating better mathematical models for measuring and assisting governments and the insurance industry in preventing terrorism future hazards was really urgent (OECD, 2005). Terrorism risk shares similar characteristics with catastrophe risk, but it also requires more complex engineering systems for risk analysis because, unlike natural disasters, it is always related to human intelligence and human intent, and therefore, far more difficult to control and prevent (Major, 2002). For this reason, several methods were applied to construct terrorism risk models, such as operations research, which includes game theory and search theory, as well as certain specialized statistical areas. According to the game theory rules, it was created a simplified model which explains the possible choices that terrorists (attacker) and government or insurance industries (defender) possess for implementing their strategies (Major, 2002). This model, named Attacker-Defender model, can be summarize in the following equation:

(1) $$EL = \Sigma_i V_i \cdot p \cdot (V_i, A_i, D_i)$$

This equation is based on a series of simplifications:

- There is a specific set of targets indexed by the letter *i*, which are numbered from one to N. Each of this target has its own value V_i;

- An attacker has total resources A_T, he has to choose a particular target and how much resource A_i to assign to the selected target;
- The defender has a maximum number of resources D_T, and he must decide the allocation of his resources D_i among the numerous possible targets;
- Attacker and defender want respectively to maximize and minimized the expected losses EL calculated through the pre-mentioned formula;
- The complete destruction of target i may occur with probability given by the formula's function $p\cdot(V_i, A_i, D_i)$.
- It is possible to use the expected value criteria until we consider the numerous values V_i as representation of agents' utilities, and as long as both sides have the same utilities (Major, 2002).

Given these assumptions and the equation, the attacker's strategy options mainly consist on the choice of the targets and the allocation of resources for the attack. On the contrary, the defender's strategies are all concentrated in the simultaneous assignment of all the resources he possesses to the all potential N targets that can be threaten (Major, 2002). In that situation, the minimax criterion[29] reveals the strategy of the defender: in fact, without knowing the attacker choices and targets, the defender will choose the strategy that minimize the expected loss (EL) considering the worst-case scenario. This means that the resulting expected loss of all the defended targets will be the same, because the defender will choose to allocate a higher part of its resources to the most important targets and smaller part to the less relevant targets (underdefended or even undefended), especially when, even in the case of certain attacks on these targets, the resulting loss is lower than the expected loss on the good defended ones (Major, 2002). On the other hand, the attacker has a specific set of M defended targets, and he wanted to maximize his attacks and therefore he has to select the optimal target. Therefore, his final strategy will be a mixed strategy in which he can choose the target he wants randomness because every target, as previously explained has the same expected loss (Major, 2002). The common game theoretic formulation assumes that both agents will act without knowing the other side's strategic choices and so, they will allocate their resources optimally in order to reach their goals. For all these reasons, it is possible to calculate the overall probability distribution of losses from a specific attack. In fact, each of

[29]The minimax criterion is a decision rule usually used in the decision theory, game theory and statistical models aimed at minimizing eventual losses for a worst-case scenario (Major, 2002).

the defended and undefended target has a probability p_i of being attacked and every targets *i* have the probability of losing its value V_i which is equal to $p_i = EL°/V_i$ (Major, 2002).

The Attacker-Defender model is particular important for its ability to describe a very complex phenomenon with a simple equation and a relatively small number of assumptions, by giving a solution, even if it is based on several simplifications, to eventual terrorists and defender strategies (Major, 2002). In reality this model appears to be very unrealistic, because it just explained how to calculate the severity of the expected loss and the probability of the attacks, without giving any information about the frequency of these hazards. There are also other limits that must be underlined:

1) It doesn't explain how to measure attack and defense resources;
2) Terroristic organization which usually influence the frequency of the attacks are not considered as part of the analysis;
3) The model only considers just one attack at a time, while in real world attacks can be simultaneously and dynamic (Major, 2002).

This means that in the activity of modelling terrorism risk, a simple analysis of probability is clearly not enough. However, the Attacker-Defender model reveals some maxims about defending targets and at the same time, it shows the way for calculating the probability distribution of losses (Major, 2002).

2.4.3 Three variables Terrorism Risk model.

In the aftermath of September 11th, the probabilistic risk analysis (PRA) was one of the major tools for assessing risks and providing information for government and insurance industry's risk management decisions (Ezell, Bennett, Von Winterfeldt, Sokolowski, Collins, 2010). PRA was also applied to terrorism risk analysis in order to have a different point of view compared to the others already applied terrorism risk management techniques. From this theoretical analysis it was developed a model which expresses terrorism risk as a function of three different variable: threat, vulnerability and consequences (Ezell, Bennett, Von Winterfeldt, Sokolowski, Collins, 2010).

The first variable, threat, is measured as "the probability that a specific target is attacked in a particular way during a specified time period" (Willis, Morral, Kelly, Medby, 2005):

$$Threat = P(\text{attack occurs})$$

Both people and organizations can represent a terrorist threat, especially when they have the intent and capability to damage a specific target. Therefore, homeland security resources are allocated in order to protect infrastructures that can be possible targets for different types of terroristic attacks (Willis, Morral, Kelly, Medby, 2005). This measure of terrorist threat is focused on specific type of attacks and targets. In fact, it is almost impossible to have a complete description of every possible combination of mode of attacks and target exposed to these attacks. Therefore, this first variable concentrates its analysis on a limited number of target and type of terroristic actions (Willis, Morral, Kelly, Medby, 2005).

The second variable is vulnerability, which is "the probability that damages, which may involve fatalities, injuries, property damage, or other consequences, occur, given a specific attack type, at a specific time, on a given target" (Willis, Morral, Kelly, Medby, 2005).

$$\textit{Vulnerability} = \text{P(attack results in damage/ attack occurs)}$$

This measure is "also the manifestation of the inherent states of the system, in terms of physical, technical, organizational and cultural features, that can result in damage if attacked by an adversary" (Haimes, 2004). The former definition is a simplification made in explaining the concept of vulnerability: in this specific model there are either successful attacks with damages or no success with no specific damages, no other options are considered (Willis, Morral, Kelly, Medby, 2005).

The third and last variable is the consequence, defined as "the expected magnitude of damage, such as number of deaths, injuries or amount of property damage, given a specific attack type, at a specified time, that result in damage to a specific target" (Willis, Morral, Kelly, Medby, 2005).

$$\textit{Consequence} = \text{E(damage/ attack occurs and results in damage)}$$

However, this measure can be affected by several uncertain factors, and therefore, because this variable is based on several assumptions, like the previous two, cannot give a 100% correct estimation of consequences in case of a terroristic attack, there will always be a small percentage of uncertainty in the measurement due to the complex and dynamic nature of terrorism risk (Haimes, 2004).

With the combination of these three variables, it is possible to give an accurate definition and measurement of terrorism risk (Ezell, Bennett, Von Winterfeldt, Sokolowski, Collins, 2010). Risk is therefore "the expected consequences over some period of time to a defined set of targets, resulting from a defined set of threats" (Willis, Morral, Kelly, Medby, 2005).

For that, given a specific threat, a particular target, and type of consequence, risk is measured such as:

(2) $Terrorism\ Risk = P(A) \times P(S|A) \times C = Threat \times Vulnerability \times Consequences$

In probabilistic terms, this equation defines risk from a specific type of attack as the unconditional expected value of damages of a certain type (Willis, Morral, Kelly, Medby, 2005). According to this definition of terrorism risk, there are two main advantages emphasized by this model, that must be underlined:

- It provides an innovative method for comparing and aggregating terrorism risk. It is also possible to compare and combined risks of particular types across diverse targets;
- Equation (2) gives a clear mapping of risk and approaches for managing and reducing terrorism risk. Indeed, risk can be managed using intelligence and active defense which are specifically focused on threats, or it can be managed thanks to the increase in surveillance and detection or other capabilities that partially eliminate vulnerabilities, or, at the end, it can be reduced by increasing preparedness and responsiveness that mitigate terrorist attacks' consequences (Willis, Morral, Kelly, Medby, 2005).

However, the three variables model has two principal drawbacks that are a great a source of uncertainties in estimating terrorism risk. Firstly, there may be errors and variabilities in the phase of estimation of the three variables, especially because it is impossible to have a comprehensive knowledge of plans and capabilities of terrorists, and this can result in certain level of uncertainty (Willis, Morral, Kelly, Medby, 2005). Secondly, it is really difficult the valuation of the terrorist attacks' consequences, since very often are based on experts' judgments that are subjective and therefore not perfectly applicable to a more objective measurement (Willis, Morral, Kelly, Medby, 2005).

2.4.4 Modelling Terrorism Risk through Social Network Analysis.

This last model, that is based on the social network analysis, was developed for better estimating terrorist attack frequency (Risk Management Solutions Report, 2012). It was demonstrated that the use of social network analysis instead of subjective experts' opinions, it is more efficient for understanding resource and constraints that basically affect terrorist

organizations, and therefore, probabilistic models can quantitatively measure attack frequency in a more convenient way (Risk Management Solutions Report, 2012).

The social network analysis model is based on the analysis and monitoring activities of terrorists' electronic communications. In fact, their communication and social network activities can be intercepted thanks to intelligence and security services and their data may be used to interdict terrorists' plans (Risk Management Solutions Report, 2012). By using quantitative social network analysis for measuring attack frequency greatly decreases the reliance of qualitative experts' judgments, providing a more affordable method that improves probabilistic terrorism modelling. Moreover, terrorists' social network analysis provides an important assistance in detecting the identity of terrorists (Risk Management Solutions Report, 2012).

Finally, social network analysis has made easier to prevent mega terrorism[30]: the more elaborate and ambitious the plain is, the more operatives and electronic communication are required to coordinate the attack. Therefore, the likelihood of interdiction increases with the complexity of the plan, but this also means that additional costs are required for improving the social network analysis in order to prevent catastrophes (Risk Management Solutions Report, 2012).

To conclude, during the last 10 years, governments and insurers have become more comfortable in the utilization of models to manage terrorism risks. Several different models were developed and implemented to meet this challenge, and multiple approaches were combined together in order to establish well-functioning risk-based methodologies (Ezell, Bennett, Von Winterfeldt, Sokolowski, Collins, 2010). The wealth of researches and development on terrorism risk has allowed to create more reliable probabilistic terrorism models based on more objective measurement instead of experts' opinions, and in addition, by using social network analysis, it is now faster and less complicated the activity of modelling terrorism attack frequency (Risk Management Solutions Report, 2012).

[30] Mega terrorism is a category of terroristic activity that involves a large number of individuals and it is focused on organizing a devastating attack which can seriously damage the wellbeing and economy of a target country. Usually, if the attack has success, it involves enormous losses in terms of fatalities and property damages.

2.5 The importance of hedging against Terrorism Risk

The last section of chapter two is mainly focused on giving a practical explanation about the importance of hedging techniques against terrorism risk, and therefore, their usefulness in companies and nations' recovery process. In order to achieve this goal, the section is divided into two sub-section, in which firstly, a cost-benefit analysis of long and short-term strategies implemented by governments (both practical and military strategies and financial and insurance measures) which allow a fast recovery of the society is presented, and secondly, all major benefits of hedging techniques and costs in case of absence of coverage policies are underlined.

2.5.1 Cost-benefit analysis of counterterrorism policies.

Terroristic activities have multiple roots and effects, and they especially affect the economic development and well-being of a country (Gold, 2004). It is a complex phenomenon that required a wide range of tools to control it, from military security measures, to diplomacy, until economic and social policies. In addition, terrorism greatly impacts nations with high level of poverty, inequalities and strict limits in the amount of capital which can be invested in order to improve preventing and recovery measures. Terrorist incidents usually impose very high direct costs to individuals and communities and even higher indirect costs (Gold, 2004). While the first group can be measured as the loss in terms of human life and economic value, the second one, is a more subjective measure that is strictly related to the changes in the mindset of the victims, by creating a continuous sense of fear and insecurity which reduces people well-being, and therefore, the indirect consequences are even worse than the direct ones (Gold, 2004). Indeed, when terrorism persists in a specific area for a long period, all these costs immensely increase, and population and regions can heavily suffer significant economic and human losses (Gold, 2004).

For this reason, countries must fight terrorism and use part of their resources to implement short and long-term plans for maintaining good standard of life for their citizens and for allowing a constant economic development (Gold, 2004). As previously said, the most common practical strategies implemented by governments can be divided in two groups, with both having their specific benefits and costs (usually long-term strategies are the ones with higher implementation costs, but also higher advantages):

1) Short-term preventive strategies, which are mainly based on pre-emptive disruption of already planned terroristic attacks and on protecting vulnerable targets;
2) Long-term preventive strategies, aimed at setting norms and new insurance and reinsurance policies to delegitimize terrorism, and moreover, social and political measures for reducing motivations for being part of these radical and violent groups. Finally, governments must implement economic strategies for accelerating community recovery (Bjorgo, 2013).

However, a cost-benefit and risk analysis are required in order to understand the effectiveness of these strategies, and moreover to provide an explanation of what are the strengths and weaknesses of government strategies and how they can be improved (Mueller, Stewart, 2011). It is fundamental to define what is the benefit of a security measure, and how it can be calculated. It is a function of three different variables:

(3) *Benefits* = (probability of a successful attack) × (losses sustained in the successful attack) × (reduction in risk)

With equation (3), it is taken into account the cost effectiveness of enhanced security expenditures and measures in order to avoid and decrease the probability of successful terrorist attacks (Mueller, Stewart, 2011). In addition, it specifically considers the effectiveness of the new security measure implemented (especially in the aftermath of September 11th), in terms of reduction in risk exposure and therefore, in decreasing the amount of losses sustained in case of successful attacks, including both fatalities and property damages, both direct and indirect consequences, and all possible psychological and political effects (Mueller, Stewart, 2011). For this reason, because the reduction in risk is expressed as the degree to which the new security measures have decreased the likelihood of successful terroristic attacks, it is fundamental an historical analysis about the effectiveness of previous security strategies to better understand the total improvement and how much they can still be improved (Mueller, Stewart, 2011).

To conclude, the cost-benefit analysis is particularly interesting because of its main results: first, it demonstrates that long-term security strategies (new insurance and reinsurance policies, development of innovative and more efficient terrorism risk models, or new anti-terrorism legislation) are far more effective that short-term plans especially in terms of benefits they could provide to populations: a new sense of security and wellness restauration (Mueller, Stewart, 2011). Secondly and finally, political and bureaucrats pressure basically force government to drastically increase the amount of expenditures in security measures

against terrorism risk, that in several cases, appear to be useless and just an additional expense particularly considering the small amount of benefits reached with some of these anti-terrorism measures (Mueller, Stewart, 2011). This political pressure usually happens in countries that has been target of terroristic activities during the past decades: the U.S. for example, has enforced one of the biggest and most expensive anti-terrorism network in the world which very often does not provide enough benefits compared to the immense costs sustained by citizens (Mueller, Stewart, 2011).

2.5.2 The usefulness of Terrorism Risk coverage techniques.

Despite the pre-mentioned expenses in developing more effective and reliable terrorism risk measures, its hedging practices have particular relevance not only for the wellness of citizens and for the security of the community, but also for the economic actives of all multinational and national firms (Mazzarella, 2005). Not only public entities are terrorists' targets, even corporations can be habitually targets of extremist organizations, and therefore, they may face a serious threat which negatively affects international commerce and business (Mazzarella, 2005). Indeed, global terrorism has very high costs for multinational enterprises and cannot simply be ignored; on the contrary it must require the development of anti-terrorism measures. Therefore, the primary benefits of models and policies aimed at hedging terrorism risk are the reduction of costs and the stabilization of international business for companies (Mazzarella, 2005). There are several costs that, without a reliable system of security measures for covering terrorism risk, can affect firms' performances and economic stability:

1) Global supply chain costs, which is especially vulnerable to terrorist attacks. Therefore, companies must spend part of their budgets in improving security systems otherwise they can incur in even more consistent costs and losses due to the risk of delay or disruption of their supply chain in case of terroristic attacks. These expenditures may also have the positive benefit of driving efficiency into the supply chain, as well as improving the efficiency of inventory techniques (Mazzarella, 2005);
2) Reduced direct investment and operations in high risk areas. Without appropriate terrorism risk management strategies, a large number of international firms may reduce their capital investments and business operations in countries or geographical areas with high level of terrorism risk. This may lead to reduce international

commerce and business and it also blocks the possibility to exploit all economic opportunities and to create fruitful alliances with foreign companies (Mazzarella, 2005);

3) Inefficient personnel decisions, which are usually taken by multinational firms in presence of terrorism causes. For this reason, personnel decisions may impose unintended and long-term costs on a firm, such as the expatriation of the activities to foreign countries because of the high presence of terrorism risk. This will lead to additional costs in constructing other subsidiaries, hiring a new qualified staff and in recreating a company interpersonal network (Mazzarella, 2005);
4) Political risk insurance[31]. It is a risk that multinational corporation face in case of long-term projects in unstable developing countries, which are particularly susceptible to political risk. It is essential a governmental program (as the U.S. has made with the introduction of the Terrorism Risk Insurance Act) to alleviate the market problems due to political risk insurance and to increase the amount of risk insurance available to all business (Mazzarella, 2005);
5) Transaction costs[32]. In fact, excluding terrorism risk from insurance policies generates a large amount of transaction costs that outweigh the benefit derived from not charging a higher insurance premium because of the exclusion of terrorism risk from the policy. It appears to be more efficient for insurance companies to include terrorism risk in their policies in order to decrease transaction costs (Thomas, 2003).

In addition to this list of avoidable costs for multinational firms, there are other more generic benefits which affect the entire community due to the practice of hedging terrorism risk (Willis, Al-Shahery, 2014). The phase of recovery from a terroristic attack always start from a microeconomic point of view that is basically the restart of companies' activity. With government assistance, the process is faster and more efficient due to several factors (Willis, Al-Shahery, 2014):

1) Firms can quickly compensate their losses if there is an accurate insurance program (such as TRIA for the U.S);
2) Litigation costs are reduced due to the collaboration with governmental agencies;

[31] Political risk is defined as "the potential loss of one's investment in or managerial control over a foreign asset because of instability and political changes in the host country" (Mazzarella, 2005).

[32] Transaction costs are defined as expense incurred when buying or selling a good or a service.

3) Rebuilding decision cannot be distorted by private market because they are controlled by public entities, and therefore money is spent according to a specific recovery plan (Willis, Al-Shahery, 2014);
4) Collaboration with governments greatly increase the level of security, which is a typical public goods[33], and this can lead to a positive shift in people mindset, not anymore frighten by terrorism (Gold, 2004).

To conclude, there are an immense range of benefits both for multinational firms and governments in hedging against terrorism risk, which far outweigh the costs. In addition, because multinational companies will always continue to operate on an international scale they must develop their own security systems for minimizing the eventual losses and their terrorism risk exposure (Thomas, 2003). Therefore, to achieve this complicated goal, a collaboration between public entities and private ones is required, in order to provide a continuous flow of information that can greatly help the activity of measuring, preventing and hedging this threat (Mazzarella, 2005).

2.6 Conclusion

The careful analysis made in chapter two has given several important results that has to be underlined. First, it is fundamental to specify the great importance that governmental insurance and reinsurance policies had during the economic recovery phase in the aftermath of September 11th (Webel, 2013). It is definitely clear how much is important the role of governments in hedging against an immense threat as terrorism risk, and therefore, an efficient collaboration between national institutions and private market is the base for a continuous and stable economic development, and moreover it is the faster way to restore citizens well-being (OECD, 2005). Unfortunately, even governments have their own limits of actions, and there are some drawbacks in a continuous intervention. This is the reason why private insurance market must find their own alternative solutions to prevent, control and mitigate the effects of terrorists' attacks without relaying too much on governmental actions (Riley, 2016 and Bruggeman, 2007). These tailor-made solutions are the second main result of the chapter, in fact, they provide alternative techniques in covering terrorism risk, and several benefits than conventional insurance and reinsurance policies cannot

[33] A public good is defined as "a product that an individual can consume without reducing its availability to another individual and from which no one is excluded" (OECD, 2005).

furnish (Bruggeman, 2007). However, a large part of them are still today not implemented in the correct and efficient manner that private market requires, and therefore, they should be better studied for improving their capabilities in mitigating terrorism effects and providing more benefits to their owners (OECD, 2005). Anyway, in order to facilitate the application of both conventional and unconventional insurance tools, it is absolutely required the help of reliable and effective models for measuring terrorism risk (Karolyi, Martell, 2006). In conclusion, the last result of this chapter emphasized the enormous importance of modelling terrorism risk for understanding frequency and severity of future attacks. Because of its unpredictability and dynamic nature, innovative models base on more sophisticated technologies and less dependent on experts' judgments, have been developed for avoiding tragedies such as September 11th (Ezell, Bennett, Von Winterfeldt, Sokolowski, Collins, 2010). Most of these models are based on a continuous flow of information between multinational firms and governments thanks to a strict private-public collaboration which is now giving a great help in the war against terrorism, and it is seems to be the right path for defeating this threat (Mazzarella, 2005).

Chapter 3. Evolution of Terrorism Risk Management in the U.S. Airline Industry after September 11th

3.1 Introduction

Chapter three provides an extended analysis of the main consequences and changes happened in the U.S airline industry after the terroristic attacks of September 11th, especially related to the airline risk management policies. The analysis is focused on the U.S. aviation industry because it has experienced the highest negative effects of 9/11 events, by being directly hit by the four hijacking, and therefore, it has required a more radical federal intervention for mitigating the situation of crisis already started in the previous decade (Jorion, 2012 and Rose, Blomberg, 2010).

Consequently, the chapter in divided into four sections. The first section examined the historical background of September 11th, underling the numerous conflicts between OECD countries and Muslim states, and then it describes the macroeconomic consequences of 9/11 (Kibble, 2002 and Rose, Blomberg, 2010). The second section instead provides tables and charts in order to understand the background situation of the U.S. airline industry and then, it illustrates the main consequences of the terroristic attacks of September 11th on the U.S. airline industry by analyzing the airline demand and the market prices' changes of the U.S. aviation firms (Galeotti, 2006 and Drakos, 2004). The third section highlights the importance of creating new and more effective risk management practices for hedging against terrorism risk, and thereby, it introduces all the major anti-terrorism policies developed by the U.S. aviation industry in the aftermath of 9/11: The Aviation War Risk Insurance Program, the new Airline Security Risk Analysis framework and the pre-boarding and in-flight airline security measures (Elias, Tang, Webel, 2014 and Cha, Ellingwood, Shafieezadeh, 2015). Finally, the last section of the chapter provides the cost-benefit analysis of some of the principal anti-terrorism airline measures applied by the U.S. aviation industry after September 11th, in order to demonstrate the intrinsic relation between the airline risk management practices and company value and their real effectiveness in hedging against terrorism risk and in increasing the American airline business value (Stewart, Mueller, 2013 and Carter, Rogers, Simkins, 2006).

3.2 Background and principal considerations on the terrorist attacks of September 11th

The section gives an historical background of the terrorist attacks of September 11th and moreover it accurately explains the main consequences of this tragic event. It is divided into two subsections where, first of all, all plausible economic, religious, cultural and political reasons behind the 9/11 disaster are analyzed in order to give a more comprehensible context of that period. The clash of religions between Islamism and Christianity is one of the main arguments. Secondly, the latter subsection introduces the Economic Consequences Analysis Framework, which is particularly useful in understanding the total economic impact and macroeconomic consequences of 9/11 attacks.

3.2.1 Historical analysis of the terrorist attacks of September 11th: main reasons behind the disaster.

The events of September 11th were a turning point in the worldwide history. In fact, the OECD countries, guided by the U.S.A, launched a military campaign in Afghanistan in order to find and arrest Osama bin Laden, the Islamic leader of the terroristic organization Al-Qaeda[34], and this action has begun the "War on Terror" (Kibble, 2002). Moreover, Government intervention became fundamental in order to provide more effective insurance programs and risk management procedures to avoid similar catastrophes. Therefore, the events of September 11th have led to a stricter collaboration between private and public sector especially about themes such as insurance, security and forecast of risks (Carter, Simkins, 2002).

For a better comprehension of this tragic event, a background analysis must be done in order to underline the principal reasons that may have led to the terrorist attacks. These motives can be basically divided into three main groups (Kibble, 2002):

1) Military intervention of OECD countries in the Middle East in several occasions during the twentieth century;
2) Economic and socio-cultural reasons related to the advent of Globalization, which eventually spread western culture and mindset in the Islamic states;

[34] Al Qaeda was successively defined a "terroristic group" by the European Union (EU) and the North Atlantic Treaty Organization (NATO) after the numerous attacks against civilian and military targets.

3) A continuous clash of religions between Islamists and Christians due to a substantial difference in values and believes and also, the unresolved past conflicts for which no definitive solution was ever found allowing the peaceful coexistence of both religions (Kibble, 2002).

Starting with the first point, the 20th century was a turbulent period in the Middle East because of the numerous conflicts that have interested this specific region and have requested the military intervention of Western countries, especially the U.S., which have played a vital role in the NATO military campaigns. The first problem emerged when OECD countries, fronted by the U.S., supported the creation and the expansion of the Jewish state of Israel in 1948, which has led to the subdivision of the Palestine territory in two different independent states, one Arab and one Jewish (Kibble, 2002). This solution promoted by the United Nations[35] was formally accepted by the Jewish Agency[36] but entirely rejected by the Arab leaders. Therefore, once Israel declared its independence in 1948, the first Arab-Israel war started and even today no peaceful agreement has been reached. In this situation, the Western countries support to the Israel cause, was seen such as an act of war against the Islamic states and therefore a crime that must be punished (Kibble, 2002).

"…The creation and continuation of Israel is one of the greatest crimes, and you are the leaders of its criminals. And of course, there is no need to explain and prove the degree of American support for Israel. The creation of Israel is a crime which must be erased. Each and every person whose hands have become polluted in the contribution towards this crime must pay its price and pay for it heavily..." (Bin Laden, 2002).

In addition, a factor that even more spoiled the Western – Middle East states relations was the Gulf War of 1991 after the Iraq invasion of Kuwait happened during the previous year (Carter, Simkins, 2002). In that occasion, a coalition of Muslim Middle Eastern and OECD countries was created in order to jointly defeat the Saddam Hussein's[37] army. Several economic sanctions were imposed on Iraq, starting with a full trade embargo except for items

[35] The United Nations (UN) is an intergovernmental organization which promote international co-operation and help to maintain international order and peace.

[36] The Jewish Agency is the largest Jewish nonprofit organization which has played a vital role in the foundation and development of Israel, promoting a mass immigration of Jewish in this country after its foundation.

[37] Saddam Hussein was the Iraq dictator from 1979 until 2003 and he seems to have strict relationship with Islamic extremist groups and more in particular with the Al-Qaeda organization and Osama bin Laden.

of humanitarian necessity (food, water and medicines). In that particular moment, the most extremist Islamic faction clashed against the moderate Muslim coalition, accusing them of having been corrupted by Western distorted values and faith, significantly increasing their resentment towards the U.S. and the other OECD countries. Moreover, after the end of the Gulf War, the U.S. decided to maintain a contingent of troops stationed in Saudi Arabia in order to preserve order in these regions, but this decision was seen as an act of provocation and an affront towards the Islamic people as a result of their proximity to the holiest place for the Islamic faith, the Mecca (Kibble, 2002).

The second point which has exacerbated the tension between West and Middle East states was the advent of Globalization, which has definitely changed people mindset (Lewis, 2003). In fact, several Islamic leaders have underlined the rapid decline of Arab culture and religion due to the dominance of Occidental countries which have spread their modern ideas and culture in the Middle East, influencing the socio-cultural values of these populations. Furthermore, during the last fifty years, the numerous Globalization's effects have posed several acute problems for Islamic rules, both emotional and practical, such as the loss of people religious identity and the extremely high difference of living standards between Islamic and Catholics states, with the latter far more developed and richer (Lewis, 2003). Still today, Islamic rulers struggle to find practical solutions for these problems which allowed to rebuild their leadership and the renaissance of the Islamic culture and religion (Lewis, 2003).

The third main reason that has led to the tragic event of September 11th has to be researched in the concept of clash of civilization, specifically defined by Samuel Huntington[38] in 1993 as a "conflict between world's different cultures and religions" a not between countries. In his master peace, the "Clash of Civilizations?", he precisely states the harmfulness of the Islamic extremist movements for the world peace (Huntington, 1993). Western cultural and religious values are completely different from the Islamic ones; liberalism, constitutionalism, equality, individualism and free markets are all foreign concepts for Middle East civilization, and therefore, they may involve conflicts for obtaining the cultural predominance and deter the reciprocal influence, even if it can result in substantial advantages for both societies (Kibble, 2002). Moreover, for centuries, a continuous and unresolved clash of religions emerged between Christians and Muslims, basically because

[38] Samuel Phillips Huntington was one of the most important experts in political scientist and director of Harvard's Center for International Affairs.

both groups assert the truth nature of their faith, considering it the only universal religion, and therefore, that any other creed is, by definition, erroneous (Kibble, 2002).

At the end, all these economic, socio-cultural, political and religious motives, plus the military threat that OECD countries may posed on the Muslim states' sovereignty, have allowed the development of extremist Islamic movements whose final aim was to hardly strike Western countries in order to demonstrate their power and free their people from Western states' compulsion and corrupted values (Kibble, 2002).

3.2.2 Considerations and consequences of September 11th on the worldwide economy.

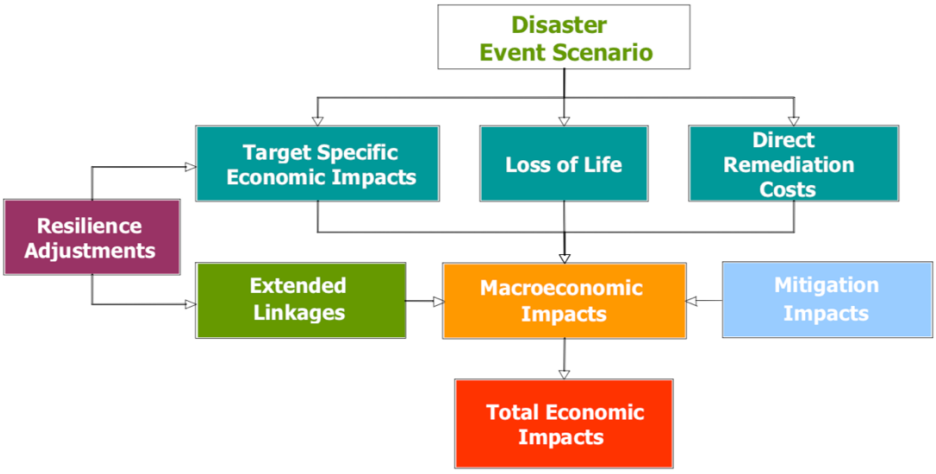
The tragic event of September 11th, 2001 was the worst terroristic attack in worldwide history and it has caused the death of 2996 persons and over 6000 injuries in the four different attacks and more than 32,5 billion dollars of property damages (Jorion, 2012). The 19 Al-Qaeda terrorists have hijacked four passenger flights of two major U.S.A airline companies, United Airlines and America Airlines, and crashed two of them, the American Airlines Flight 11 and United Airlines Flight 175, into the North and South towers of the World Trade Center in New York City, causing the collapse of both towers after having been seriously damaged by the impacts, then a third flight, the American Airline Flight 77, was crashed into the U.S. Department of Defense, the Pentagon, in Virginia, causing several damages on the building's west part, and a last airplane, the United Airlines Flight 93, which has never reached its target (which is still today subject to several speculations) because of a strong passenger resistance, was crashed it into a field in Pennsylvania (Jorion, 2012 and Rose, Blomberg, 2010). On that day, when the Twin Towers collapsed as a result of the structural damages they have suffered during the attacks, 2750 persons died; other 184 persons were killed by the passenger flight that crashed into the Pentagon, and finally, other 43 victims on the United Airlines Flight 93, which didn't reach the estimated target (Jorion, 2012 and Rose, Blomberg, 2010)[39].

The tragic event of 9/11 has involved negative economic consequences for both the U.S. and the worldwide economy, and therefore, the year 2001 was a very difficult and turbulent year

[39]Some information about the number of victims are from BBC News and New York Time website (http://www.bbc.com/; https://www.nytimes.com/ (day of access: September 16th)).

characterized by numerous enterprise scandals[40], the headwinds of a recession and in addition, the tragedy of September 11th (Blomberg, Hess, 2009). In order to understand the full consequences of this event, it was developed an expanded framework which was able to accurately calculate the overall outcome of 9/11 terroristic attacks and more in general of man-made or natural disaster (Blomberg, Hess, 2009). In fact, instead of just considering the direct economic impacts, losses of lives and direct remediation costs related to a disaster, this specific scheme also takes into account additional elements such as the society resilience capacity, the numerous extended linkages and the mitigation impacts which can basically change the final macroeconomic impact and therefore the total economic impacts of a disaster's scenario (Rose, Blomberg, 2010).

Figure 6. Economic Consequences Analysis Framework.



Source: Rose A. Z., Blomberg B. S. (2010), "Total Economic Consequences of Terrorists Attacks: Insights from 9/11", Published Articles & Papers, Vol. 16, Issue 1, pp. 1-12.

This framework considers all types of resilience actions which can mute the initial shock and speed up the recovery process. Moreover, it introduces the importance of the extended linkages which refers to behavioral reactions to different shocks (such as fear of doing a specific activity because of a traumatic event recently happened) and mitigation and interdiction actions and costs which have the goal of reducing the negative effects of a disaster (Rose, Blomberg, 2010). Eventually, the sum of all these components influence the macroeconomic impact of a disaster event scenario and therefore, the overall economic

[40] Some American companies such as Enron, the Pacific Gas and Electric Company and WorldCom have experienced a period of crisis in the year 2001 that has involved in several occasions a firm state of insolvency or bankruptcy, and even fraudulent bankruptcy.

impact on the society, simultaneously giving a more accurate analysis of the system's recovery capabilities to severe shocks (Rose, Blomberg, 2010).

Therefore, as a result of the analysis made by this framework, the macroeconomic impact of September 11th was particularly relevant, and in fact, it was estimated that the total losses were in a range between 60 and 125 billion dollars, which means a decrease approximately between 0.50 and 1.08 percentage point in the U.S. GDP growth (Blomberg, Hess, 2009). Moreover, the U.S. have experienced a loss of 0.07 percentage point of their total physical assets[41], with a total amount of property damages around 30 billion dollars (Jorion, 2012). Finally, the terrorist attacks of September 11th have significantly affected the global economy, spreading fear of travelling around the world and consequently, directly impacting several sectors, such as airlines[42], travel services and insurance. The airline sector suffered significant losses due to the decrease in the air traffic in the months after the incident, especially in the last twenty days of September when the traffic plummeted by 34% and it has involved huge economic losses for airline companies (Jorion, 2012). Travel services have faced a similar period of crisis due to the tourists' fear of travelling abroad, meanwhile the effect on the insurance sector was different and more complex than previous two, and it has required the specific intervention of Governments in order to provide an effective way for hedging terrorism risk[43], because of the private sector inability and inadequacy in accomplishing this task (Jorion, 2012). The market as a whole has experienced a loss of 5 percentage points in one week, and the airline and travel sector dropped even more, while the insurance industry has risen in the aftermath of 9/11, reflecting the risk premiums increase. A high level of uncertainty and volatility was also associated to the lower values of the market in the subsequent period (Jorion, 2012).

By time, the U.S Government and the Federal Reserve were able to mitigate the negative consequences of September 11th, restoring the previous levels of wellbeing and safety in the American society. Simultaneously, the other OECD countries have implemented similar

[41] In 2001, it was calculated that the total amount of the U.S. physical assets was around 30.000 billion dollars (Jorion, 2012).

[42] The 9/11 consequences on the airline industry will be better analyzed in the third paragraph of this chapter, as it is one of the principal arguments of the thesis.

[43] The insurability of terrorism risk is analyzed in the second paragraph of chapter two.

measures to stabilize international markets, reassure their citizens about their safety and avoid a period of economic recession (Rose, Blomberg, 2010).

3.3 Economic consequences on the U.S. airline industry

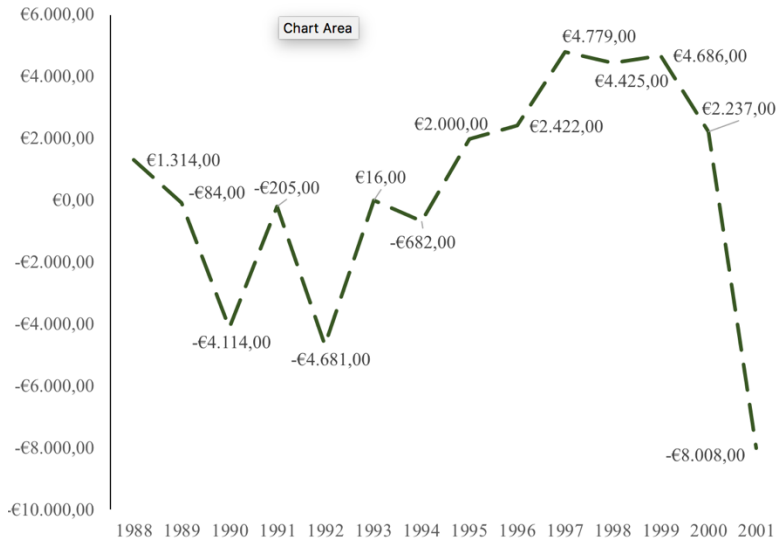
The third section is focused on giving a detailed analysis of the main consequences of the terrorist attacks of September 11th on the U.S airline industry, which was the most damaged sector in 2001. To accomplish this goal, the section is basically divided into two subsections: the first one, gives a thorough description of the most important events that has affected the aviation sector before 9/11, in order to give a more comprehensible airline industry's context. Instead, the second subsection specifically explains the impact of 9/11 on the U.S. airline companies, by focusing the attention on the analysis of the airline demand and the market price changes of the U.S. airlines' stocks. It also takes support from other relevant scholars' works, which are briefly introduced, to provide more accurate results of the total economic impact of September 11th.

3.3.1 The U.S. airline sector background before the terrorist attacks of September 11th.

The former section has underlined the September 11th terrorist attacks' huge effect on several sectors, and especially on the U.S. aviation industry (Ghobrial, Irvin, 2004). That attack on the United States had the precise intent to harm the nation in numerous ways: from fatalities and causalities among innocent people, to the disturbance of the civil air transport system and finally, to feed an international economic crisis (Looney, 2002). Consequently, in order to reach this final goal, terrorists hit one of the most important sector for the U.S economy, the aviation, which has always played a vital role in the American economic prosperity, by connecting communities and nations together for business, commerce and tourism purposes, and in addition, it employed thousands of U.S. citizens (Ghobrial, Irvin, 2004).

Once the disaster happened, the American airline industry was already experiencing a difficult situation, where many airline corporations have declared bankruptcy and many more have reported net losses in billion dollars in the last years (Doganis, 2006).

Chart 1. U.S. Airlines Net Profit between 1988-2001 in million dollars.

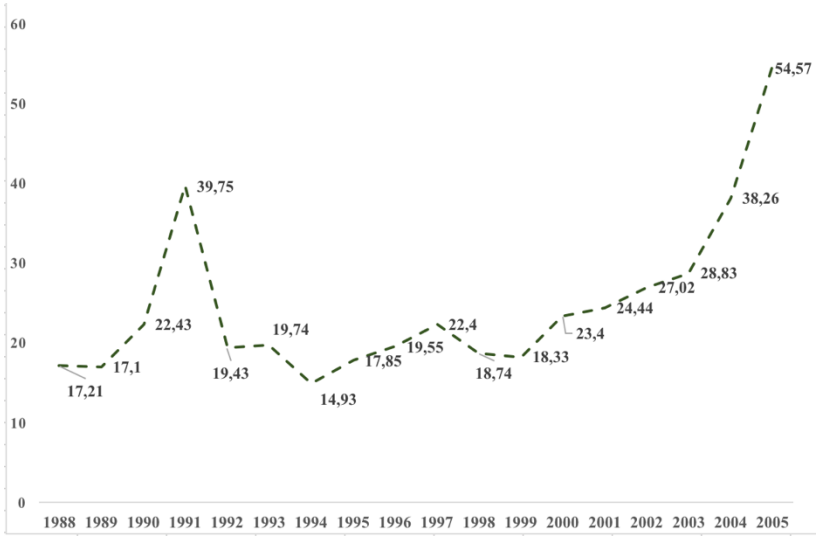


Processed by the author, data source: www.airlines.org and Airlines for America Industry Report (2018), "U.S. Airline Industry Review: Allocating Capital to Benefit Customers, Employees and Investors", pp. 1-78

Chart 1 illustrates the net profit of American airline companies between 1988 and 2001, showing the already difficult situations they were facing before the terrorist attacks of 9/11. In fact, this data demonstrated the period of crisis that airlines were facing during the Gulf War (1990-91), which has led to losses for over four billion dollars in 1990 and 1992 and very low net profit between 1989-94. Finally, before the events of 9/11, the U.S. airline firms were already experiencing a decrease in company profits, passing from $4,686 millions in 1999 to $2,237 millions in 2000 until the huge loss of more than 8 billion dollars of 2001 (Airlines for America Industry Report, 2018).

One of the main reasons, which has started the negative trend, was the increase in the jet fuel prices, due to the precedent Gulf War and during the years of the Asian crisis from 1998-2002 (Galeotti, 2006). In that period, the OPEC decreased the oil production by 1,719 million of barrels, and therefore, there was an increase in the oil price which has passed to almost 25$ each barrel and even rose above 27 dollars in 2000. More in general, the total fuel expenditure for U.S. airlines increased from 9,020 million dollars in 1999 to $14,099 million in 2000 and other 13,120 million in 2001 (www.airlines.org), and this has drastically reduced their net profits, which was partially covered with an increase in the number of layoffs in order to cut operating costs (Looney, 2002 and Galeotti, 2006).

Chart 2. Oil price in dollars per barrel between 1988-2005.

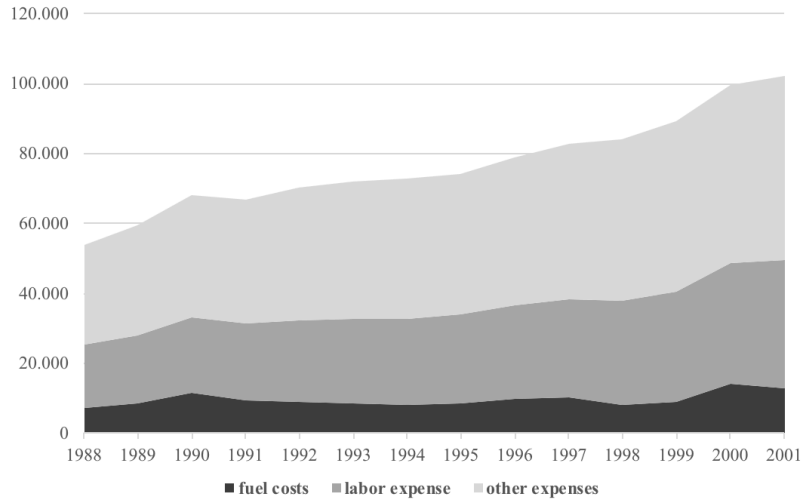


Process by the author, data source: www.airlines.org and Galeotti M. (2006), "1986-2006: Vent'anni di prezzi del petrolio", L'Italia nell'economia internazionale, Rapporto ICE 2005-2006, pp. 69-84.

Chart 2 reassumes the changes in the oil prince between 1988-2005, and it provides evidences for highlighting the increase in the aircrafts' fuel cost before the terroristic attacks of September 11th, demonstrating one of the causes that has started a three-year period of crisis for the U.S. airline companies.

The increase in fuel prices was just one of the several reasons that has led to this difficult economic situation for the U.S. airline industry (Carter, Simkins, 2002). In fact, the increase in labor costs and non-labor costs, a category of operational costs that considers all possible structural costs such as outside maintenance, non-aircraft ownership, aircraft rental and also security costs, has involved the rise of the total operating expenses of U.S. airlines, consequently reducing their economic performance (Belobaba, Hernandez, Jenkins, Powell, Swelbar, 2011).

Chart 3. Total U.S. Airline Operating Expenses between 1988-2001.



Process by the author, data source: www.airlines.org and Belobaba P… (2011), "Productivity Trends in the U.S. Passengers Airline Industry 1978-2010" …, pp. 1-76.

Notes: the unit of measurement is in million dollars.

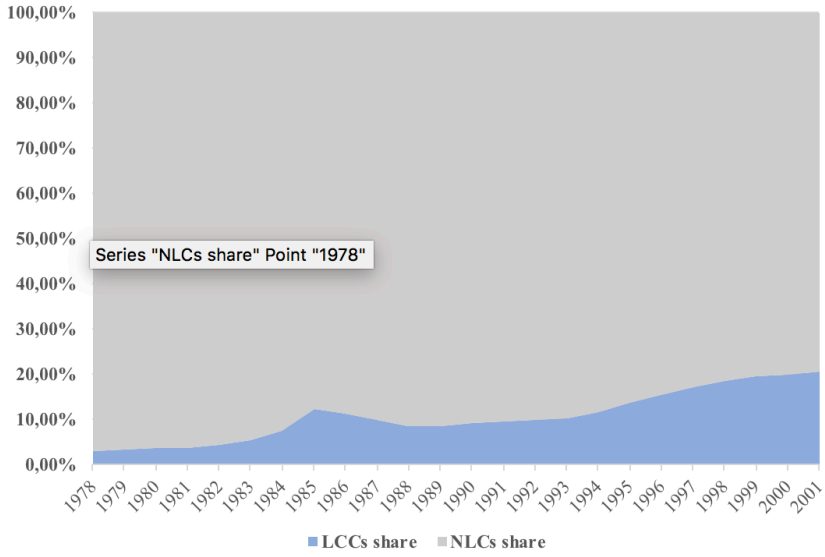
As it is showed by chart 3, the U.S. aviation industry experienced a negative trend in their net profits because of the increase of their total operating expenses due to the simultaneous growth of fuel prices, labor costs and other non-labor costs (which has experienced the higher increase in the 90s), passing from a total expense of $53,587 millions in 1988 to 102,377 million dollars in 2001.

This difficult economic situation was also related to the introduction of new regulations adopted in the past decades, which have changed the international aviation competition and seriously affected the U.S. aviation sector's economic performance (Carter, Simkins, 2002). In fact, with the approval of the U.S. Congress Deregulation Act passed in 1978, all governmental controls over fares and domestic routes were removed and for the first time, Government has given the possibility to the airline companies to operate as true businesses. Therefore, in the subsequent years, a high number of airlines were founded while the already established companies have faced a struggle to adapt to this deregulation process (Carter, Simkins, 2002). Because of the numerous complication encountered in a deregulated market, the 1980's were a less profitable period for the aviation sectors, and moreover, only one of the new airlines; the American West, succeeded, instead all the other new U.S. airlines failed. Other three well established major airlines, Eastern, PanAm, and Braniff International could

not survive to the new deregulated environment and they were forced to shut down[44]. At the end of this period, many small airlines were acquired by larger and established companies because of a starting process of consolidation within the sector (Carter, Simkins, 2002).

The second important factor was the deregulation pressure supported by the U.S. Government in the international travel between U.S. and other countries, especially with European states, which represented the second largest air travel region after America. During that period, also European Union countries have started an air travel liberalization program (started in 1987 until 1997), which was changing the European competition rules (Oprea, 2010). Furthermore, this phenomenon has led to creation and consequently expansion of low-costs companies (LCCs), which proposed different business models and pricing strategies compared to the more established national carriers (also called Network Legacy Carriers, NLCs) and seriously exacerbated the international airlines competition. Their lower cost structure allowed to obtain a growing market share and to generate operating profits, forcing the NLCs to restructure their business models in order to preserve their level of profitability (Doganis, 2006 and Belobaba, Hernandez, Jenkins, Powell, Swelbar, 2011).

Chart 4. Share of U.S. Airlines Domestic Output between 1978-2001.



Process by the author, data source: www.airlines.org and Belobaba P… (2011), "Productivity Trends in the U.S. Passengers Airline Industry 1978-2010" …, pp. 1-76.

[44] More specifically, Eastern was liquidated in 1991, Pan Am declared bankruptcy in the same year and Braniff International ceased its operations in 1982 shortly after the Deregulation Act of 1978 because of its inability to face the new competition (Carter, Simkins, 2002).

Chart 4 shows the American[45] low-cost carriers growth during the 80s and 90s. The surviving low-cost airlines established after the Deregulation Act in 1978, still accounted for a very short percentage until 1991, around 7%, but they steady rose until 2000 capturing almost the 20% of the total U.S. Airlines domestic output. This phenomenon has affected national carriers' performance as previously explained, especially concerning short flights' profits, where a large part of passengers decided to choose flights handled by low-costs companies in order to save money (Belobaba, Hernandez, Jenkins, Powell, Swelbar, 2011).

In conclusion, the impact of all these previous events has created an unstable U.S. airline industry even before the terroristic attacks of September 11th, 2001. Therefore, the impact of 9/11 was overstated by this already fragile environment, seriously worsened the American aviation sector's period of crisis, which has led to an effective loss of almost three years of growth (Doganis, 2006).

3.3.2 The impact of 9/11 on the U.S. airline business.

The terrorist attack of September 11th has created a large variety of economic and political effects on several industries and moreover, it has involved a renewal of Government protocols which enforced new permanent regulations on issues like national security and international relations (Drakos, 2004 and Virgo, 2001). The 9/11 was just the beginning of the most challenging years (almost a decade) in the airline industry's history, especially considering the weak financial position that it was already experiencing in last years of the twentieth century. The total U.S. domestic aviation market lost almost $142 billion in the period between 2001-2010 and the employment levels drastically declined with the U.S. company profits, passing form more than 520,000 workers in 2000, to 444,700 employers in 2003 (they had fallen by 14.6%), until 378,100 workers in 2010 (IATA Report, 2010).

[45] In this chapter, the word "American" is used only for intending the U.S.A. country and not the entire continent.

Table 3. Global Aviation Industry figures after the impact of September 11th.

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Revenues ($ billion)	329	307	306	322	379	413	465	510	564	482	554
Passenger growth %*	8.6	-2.7	1.0	2.3	14.9	7.0	5.0	6.4	1.5	-2.1	7.3
Passenger numbers (millions)	1,828	1,793	1,792	1,849	2,064	2,211	2,328	2,497	2,507	2,479	2,681
Crude oil price (Brent) $/b	28.8	24.7	25.1	28.8	38.3	54.5	65.1	73.0	99.0	62.0	79.4
Jet Fuel price $/b	36.7	30.5	29.1	34.7	49.7	71.0	81.9	90.0	126.7	71.1	91.4
Net profit ($ billion)	3.7	-13.0	-11.3	-7.5	-5.6	-4.1	5.0	14.7	-16.0	-9.9	18.0
Margin %	1.1	-4.2	-3.7	-2.3	-1.5	-1.0	1.1	2.9	-2.8	-2.1	3.2

Source: International Air Transport Association (IATA) Report (2010), "The Impact of September 11th, 2001 on Aviation", pp. 1-8.

Table 3 gives some information about the principal economic and financial indicators of the global aviation industry in the aftermath of 9/11. It is clear the two most affected years by the tragic incident are the closest one, so 2001 and 2002, where the total net profit of the sector decreases by 13.0 and 11.3 billion dollars respectively, and the passenger numbers are the lowest in the last 10 years due to their fear of using airplanes for travelling. By the way, also 2008 is a particularly problematic year for airlines company, due to the sharp increase of the jet fuel price which has involved a drastic reduction in companies' profits (in 2008 the global aviation industry net profit declined by $16.0 billion), even worse than the one experiences in 2001-02 (IATA Report, 2010).

According to this information, the U.S. airline industry was hit the most, experiencing a passenger traffic decline by nearly 40 percentage point in 2001 and the huge financial losses related to 9/11 have involved the liquidation of several established companies a few years later (Kim, Gu, 2004)[46]. Therefore, in order to better comprehend the magnitude of this situation, several models where developed to analyze the economic crisis that airline companies faced on that years (Ghobrial, Irvin, 2004). One of the most important models,

[46] United Airlines, US Airways, Hawaiian Airlines and National Airlines all declared bankruptcy few years after (Kim, Gu, 2004).

which has been developed by Ghobrial and Irvin with the aim of giving an extensive analysis of the total economic effects of September 11th on the U.S airline sector, is the "Airlines-Airports-Passengers Model" (Ghobrial, Irvin, 2004).

This model analyzes the linkages of the three-singular factors in order to accomplish the main goal of calculating the total event impact on the aviation industry. It divides the aviation sector into three different components and it firstly, considers each one on its own, secondly the linkages between each other, and thirdly, it calculates the final effect (Ghobrial, Irvin, 2004). At the end of this analysis, the model shows how much these three distinctive factors are interrelated and hence, it tries to calculate their total contribution to the aviation sector crisis at the begging of the 2000s (Ghobrial, Irvin, 2004). One of the most significant results was the shift in customer choices about short flights: especially in the U.S. there was a decline of almost 30% of total passengers who have chosen other forms of transport instead of airplanes for short distances due to 9/11 events (Ito, Lee, 2003).

Literature has tried to calculate the September 11th economic impact on U.S. airline companies, by examining three different variables: the airline stocks, the systematic and total aviation risk and finally, the U.S. airline demand (Drakos, 2004 and Kim, Gu, 2004). The main results of this studies were that the average drop of the U.S airline stocks is more than three times bigger the average drop of non-U.S. airline stocks (53.28% compared to 17.90%), explaining the immense losses in market value terms for American companies, and moreover several U.S. companies didn't recover their precedent stock price, such as American Airlines, United Airlines (the ones that had their aircraft hijacked) and Continental Airlines (Drakos, 2004). The last result highlighted that the majority of airline stocks were associated with significant low systematic risk, where the average U.S. airline percentage of systematic risk on total risk[47] was around 12%, while, after September 11th, it has almost doubled (around 21%) and the average systematic risk percentage on total risk considering both U.S. and non-U.S. airlines passed from 10.95% to 18.85% (Drakos, 2004 and Kim, Gu, 2004).

The last factor examined was the U.S airline market demand which has suffered severe consequences after September 11th. Two famous scholars, Ito and Lee, have deeply analyzed

[47] Total risk is made by the sum of systematic risk (which is the risk that cannot be diversified because it is intrinsic in the aggregate market, but it can be hedged) and idiosyncratic risk (it can be diversified, and it is specific to a firm or an industry).

the U.S. airline demand post 9/11, and according to their main results, it has experienced a negative demand shock of more than 30%, basically explained by the decrease in the number of passengers who preferred to use other non-U.S. carriers for their international flights (Ito, Lee, 2003 and 2004). According to their data, the entire U.S. airline industry has taken more than two years for reaching the pre-September 11th demand values, thanks to the dissipation of the initial panic and fear of flying and to the introduction of more rigorous security measures which reassured people about the safety of airports and aircrafts (Ito, Lee, 2003 and 2004).

Based on these studies, the work will further focus on analyzing a sample made by some of the most important U.S. airlines (American Airlines, Southwest Airlines, Frontier Airlines and United Airlines) and non-U.S. airlines (Air New Zealand, Air France, Alitalia, British Airways and Qantas Airlines) active in that period in order to strengthen the previous studies by demonstrating the period of crisis of the U.S. airline industry happened in the aftermath of the terrorist attacks of September 11th. The sample considers some non-American airline companies in order to highlight the fact that markets are strictly integrated and hence, a single event may cause great changes in the entire network. In addition, the companies used in the sample are all from OECD countries to emphasize their close interrelation.

The study illustrates the September 11th impact on U.S. and non-U.S. aviation enterprises' revenues, a factor that is strictly related to the number of passenger, especially because, passengers' flight tickets are the only source of revenues for airlines, and therefore a decrease in company's revenues can be only related to a decrease in the number of passenger and/or a cost[48] increase. Moreover, the total number of passengers composes the airline travel demand, and therefore, by analyzing the revenues' trend is also possible to analyze the changes in the airline demand.

[48] The previous subsection (in particular chart 3) shows an extended analysis of the operating costs that U.S. airlines faced between 1988-2001.

Table 4. Post September 11th changes in airlines' revenues.

	2000	2001	2002	2003
American Airlines	**19.703,0**	**18.963,0**	**17.299,0**	**17.440,0**
		-4%	-9%	1%
Southwest Ailrlines	**5.649,6**	**5.555,2**	**5.521,8**	**5.937,0**
		-2%	-1%	8%
United Airlines	**9.899,0**	**8.969,0**	**8.402,0**	**8.870,0**
		-9%	-6%	6%
Qantas Airlines	**9.072,1**	**10.127,3**	**10.968,5**	**11.374,6**
		12%	8%	4%
Frontier Airlines	**329,8**	**472,9**	**445,1**	**469,9**
		43%	-6%	6%
Air New Zealand	**3.656,4**	**4.024,8**	**3.641,9**	**3.616,6**
		10%	-10%	-1%
British Airways	**8.940,0**	**9.278,0**	**8.340,0**	**7.688,0**
		4%	-10%	-8%
Alitalia	**5.390,9**	**5.273,5**	**4.736,7**	**4.305,8**
		-2%	-10%	-9%
Air France	**10.325,2**	**12.280,0**	**12.528,0**	**12.687,0**
		19%	2%	1%

Process by the author, data source: Bloomberg. Note: units are in millions of dollars.

Table 4 confirms the revenues' negative trend illustrated by the other scholars in the aftermath of September 11th, 2001, even if for some corporates the crisis was already started in the previous years. The decrease in revenues is basically due to the mistrust of precedent customers in the airlines' security measures which has led to the spread of the fear of flying, and hence, their decision to use alternative means of transports especially for short distances, or to pick the flight services handled by other airline companies. Therefore, the results of this analysis appear to be consistent and give some support to the previous study of Ito and Lee focused on the sharp decrease of the U.S. airline demand immediately after the tragic events of 9/11.

Furthermore, in order to provide greater evidences about the difficult situation of the American aviation industry, the work has substantially analyzed the changes in the stocks' market prices of a sample of major U.S. airline companies (American Airlines, United Airlines, Southwest Airlines, Delta Airlines, Continental Airlines and Frontier Airlines) active in 2001.

Table 5. The impact of September 11th on the U.S. airlines' stocks.

	Market value per share on Sep. 10th.	Market value per share on first day of trading after 9/11.	Price devaluation on first day of trading after 9/11 events.
American Airlines	29,7	18	-39,394%
United Airlines	30,82	17,5	-43,219%
Southwest Airlines	16,74	11,25	-32,796%
Continental Airlines	38,6	12,35	-68,005%
Delta Airlines	46,52	20	-57,008%
Frontier Airlines	15,78	6,77	-57,098%

Process by the author, data source: Bloomberg and Continental and Delta Airlines Annual Report (2001).

This second analysis provide additional evidences in accordance with Drakos and Kim's works, underlining the drastically decrease in the share market price of all major U.S. airline companies after the terrorist attacks of September 11th. The average of the U.S. airlines' price devaluation on the first day of trading after 9/11 is around 50% (more specifically 49,59%), showing a very similar result to Drakos' studies, were the average drop of the American airline stocks was around 53%, at least three times bigger than the average drop of non-U.S. airlines stocks (Drakos, 2004).

This final study has demonstrated the tough economic situation that the U.S. aviation companies were facing after 9/11. Therefore, considering the circumstances, U.S. airline companies where obliged to introduce new practical security measures and insurance hedging techniques in order to avoid other catastrophes such the 9/11 and to exit from the years of crisis (Ito, Lee, 2003).

3.4 Airlines' hedging techniques for Terrorism Risk after September 11th

The section focuses on the importance of having innovative and effective risk management techniques for hedging against terrorism risk, and therefore, the new U.S. airline companies' security measures and insurance policies appositely developed after the event of September 11th, 2001, are introduced. The section is basically divided into three subsections: the first one explains the Aviation War Risk Insurance Program which provide coverage for hostile attacks against airline companies. The second subsection examined the new Airline Security Risk Analysis framework created for identifying possible security vulnerabilities. Finally,

the last subsection gives an extended analysis of the principal airlines' technical security measures established after 9/11.

3.4.1 The Aviation War Risk Insurance Program.

In the aftermath of September 11th, the U.S. aviation companies faced a difficult situation due to the worldwide cancellation of third-party liabilities war risk coverage in the insurance market and therefore there was a particular high increase in the costs of other possible war risk insurance (Elias, Tang, Webel, 2014). To solve this problem, the U.S.A. Government intervention was required, and it decided to expand the federal Aviation War Risk Insurance Program in order to guarantee to the American airlines the requested insurance coverage which was not anymore supplied by the commercial insurance market (Borghi, 2015 and Elias, Tang, Webel, 2014). With this intervention, the commercial insurance market has reached a phase of stabilization and a large number of airlines could again purchase a war risk coverage from private insurers (Elias, Tang, Webel, 2014).

Basically, the aviation war risk insurance is a kind of insurance policy which provides hedge for all type of hostile acts against air carriers, such as sabotage, hijackings or other terroristic actions. Usually, aviation corporations cannot operate without the pre-mentioned insurance due to the fact that aircraft loan and lease agreements obligatory demand for this insurance and in addition, some countries require the war risk insurance as a basically condition for allowing airlines to operate in their airspace and airports (Elias, Tang, Webel, 2014).

The first federal intervention was required due to the growing concerns over terrorist hijacking activities during the 70s and 80s. On that occasion, the Federal Aviation Administration (FAA)[49] decided to expand the federal aviation war risk insurance coverage due to the impossibility for private insurers to provide it at reasonable rates (Elias, Tang, Webel, 2014). Therefore, the U.S. Government has provided a new aviation war risk insurance as an emergency response because of the ongoing Middle East crisis, charging a price that was almost twice than the one prior to the hijackings, but definitively less expensive than what private insurance market would have requested considering the hijackings (Elias, Tang, Webel, 2014).

[49] The Federal Aviation Administration is the U.S. national authority that regulates the U.S. civil aviation, which includes several activities such as the construction and operation of airports, air traffic management and protection of U.S. aircraft during the two phases of launch and re-entry in U.S. airspace.

In the period before September 11th the federal aviation war risk insurance was basically provided and issued without premium under specific indemnification agreements with the U.S. Department of Defense (Elias, Tang, Webel, 2014). According to these agreements, the U.S. Defense Department would have reimbursed the Federal Aviation Administration in case of incurred losses and paid out by the specific insurance fund. Therefore, the premium war risk insurance became available only for particular routes or destinations in conflict areas, as it happened in the Gulf War in 1990-91 (Elias, Tang, Webel, 2014).

In the aftermath of 9/11, because of the unpredictability of the event, insurers decided to cancel third-party liability war risk coverage for aviation companies and consequently increases the premiums for the other possible war risk insurance. Hence, to solve this situation, the U.S. Government has passed the Air Transportation Safety and System Stabilization Act in 2001, basically expanding the airline insurance coverage to include acts of terrorism (Elias, Tang, Webel, 2014 and Borghi, 2015). In the following years, the new FAA Aviation War Risk Insurance program was extended other times, as previously happened with the Terrorism Risk Insurance Act[50] of 2002. The new program mainly provided a full coverage to 44 different U.S. airlines which constituted about 99% of the revenue passenger miles (RPMs)[51] (Borghi, 2015). This kind of insurance coverage varied from a vast range between 100$ million to 4$ billion for each aircraft, with an average coverage of 1.5 billion dollars. All the premiums paid by airline companies are collected in the Aviation Insurance Revolving Fund, which was appositely created for payments in case of incurred losses (Borghi, 2015).

In accordance with the statute, the FAA Aviation War Risk Insurance program offered a coverage which begins with the first dollar of loss and it aims at reimbursing the 100% value of losses. Moreover, it incorporates the third-party was risk liability, the hull insurance and the comprehensive liability insurance and finally, it provided coverage for a vast series of hostile actions and risks (Elias, Tang, Webel, 2014):

1) War, invasion, civil war, revolution, insurrection, or any other possible attempt at usurpation of power;

[50] For having more information about the Terrorism Risk Insurance Act view the second section of chapter two.

[51] The revenue-passenger-miles is a measure used by airline companies in order to calculate the number of miles traveled by paying passengers. It is usually an airline traffic statistic.

2) Hostile detonation of some kind of war weapons, which also includes atomic or nuclear weapons;
3) Any act of damage made by one or more persons that might have political or terrorist purposes;
4) Any possible action of sabotage or hijacking against aircraft;
5) The detonation of weapons or explosives devices o aircrafts.

In summary, the U.S. Government intervention based on the introduction of the new FAA program was one of the most significant and effective risk management measures applied to the U.S. airline sector which has allowed a faster exit from the period of crisis that the industry was facing at the beginning of 2000s (Borghi, 2015).

3.4.2 The Airline Security Risk Analysis framework.

For the modern society, civil aviation is one of the most important sector due to its relevance in global commerce, travel and tourism activities, and this is the reason why in the last fifty years it has become a prime target for terrorist activities. Consequently, its protection must be ensured for allowing the continuity of commercial air transport (Carter, Rogers, Simkins, 2006).

Therefore, after the events of September 11th, the U.S. Congress has definitely understood the importance of developing new risk analysis framework and simultaneously improving the preexisting ones for having better estimations of the possible threat scenarios and hence, the possibility to apply the best mitigation options and security measures to reduce the negative events' incurred losses (Weiss, Maher, 2008). Thereby, a large number of risk management methods were proposed and developed to solve the challenge of modelling and assessing the real counterterrorism measures' effectiveness applied to the U.S. airline industry. More specifically, the new risk management frameworks have to assist companies in the activity of efficient allocation of limited budgets for enhancing airlines security against possible future terroristic attacks (Poole Jr, 2008 and Carter, Rogers, Simkins, 2006).

Consequently, to reach these goals, a new risk management framework for U.S. aviation industry was developed after the events of 9/11: The Security Risk Analysis framework (Cha, Ellingwood, Shafieezadeh, 2015). This framework is composed by five main components:

1) Scenario Identification;

2) Consequence and Criticality Assessment;
3) Security Vulnerability Assessment;
4) Threat Likelihood Assessment;
5) Life-cycle Cost Assessment.

This separation of the risk analysis into five different phases basically allows a better estimation of key risks contributors, identification of the most relevant parameters which increase the level of uncertainty and it enhances the analysis of those components in order to give better solutions to the airline industry (Cha, Ellingwood, Shafieezadeh, 2015).

The first step of the Security Risk Analysis framework, the activity of scenario identification, is based on calculating plausible threat scenarios[52] of terrorist attacks against the airline sector. In this first phase, the set of all possible threats is reduced to a manageable number of realistic threat scenarios. Historically, the two-major threats for airline companies where the detonation of conventional explosives in the airports or aboard a carrier, and the aircraft hijacking for suicide terrorist missions. The scenario identification phase must be conducted with extremely high accuracy because screened out plausible scenarios may lead to errors and uncertainty in the final risk analysis valuation (Cha, Ellingwood, Shafieezadeh, 2015).

The second phase is the consequence and critical assessment in which they are calculated the total amount of losses that can incur in case of successful terrorist attacks. Losses that can be estimated in terms of human casualties, injuries, environmental damages, economic and social impacts and other indirect or secondary damages due to business interruption and the involvement of feelings of fear and insecurity that can affect financial markets (Cha, Ellingwood, Shafieezadeh, 2015). Therefore, it is fundamental to provide the most effective losses quantification considering all the pre-mentioned dimensions, the complexity of the systems and all the possible interactions among the different losses' components. The crash of a passenger airplane for example, has several immediate consequences, such as fatalities and economic losses due to property damages (loss of the aircraft), but it also experiences indirect and additional costs due to a reduction in the air travel demand or/and a temporary shutdown of the airports in the immediate period after the terrorist attack (Cha, Ellingwood, Shafieezadeh, 2015).

[52] Threat scenarios are essentially unique combinations of key assets and threat types. Threat types are the possible threat imposed by the attackers such as explosives, biological weapons or cyber-attacks (Cha, Ellingwood, Shafieezadeh, 2015).

The security vulnerability assessment is the third step and it is focused on the probability estimation of terrorists' successful attacks against a specific target. Eventually, the calculated probability is combined with the estimated potential losses if the attack has success and it finally gives the total expected losses related to one specific threat scenario (Cha, Ellingwood, Shafieezadeh, 2015). Thereby, there are particular defense actions for stopping a terrorist attack: firstly, commercial airlines and airports create a perimeter with different sequences of security zones and secondly, they have a series of defense actions that basically consist of three steps in a precise sequence. Detect the attackers, engage him ones it is recognized and finally, neutralize the opponents (Cha, Ellingwood, Shafieezadeh, 2015).

The fourth step is the threat likelihood assessment, where aviation companies' risk analysts model the attackers' decisions making process in choosing among their possibilities at each different phases of the strikes. In summary, terrorists' preferences may be represented by the use of utility functions, that are particularly important in ordering all the available alternatives for the attackers. Because terrorists will make decisions in order to maximize their expected utility, they will choose the most effective attack profile, threat scenario and target to attack. Therefore, the airlines' risk analyst activity is focused on estimating their best option in order to provide the best possible defense actions (Cha, Ellingwood, Shafieezadeh, 2015).

Finally, the last phase, called life-cycle cost assessment, has the primary goal of developing the most effective risk mitigation options based on companies' limited resources. Eventually, the effectiveness of the risk mitigation option is examined under two different aspects; firstly, its ability to reduce the eventual incurred total losses after a terrorist attack, and secondly, its cost of implementation, considering that airlines and more in general companies from all sectors, have just a limited number of resources that can be deployed for mitigation strategies and security measures. In fact, it has been demonstrated from several studies that not all the risk mitigation actions implemented by air carriers are cost-effective and therefore they need to be enhanced or changed[53] (Cha, Ellingwood, Shafieezadeh, 2015).

In conclusion, managing terrorism risk is far more difficult than natural hazards because of its relation to the human unpredictable nature. This model appear to be very effective for airline companies due to the fact that it basically calculates for each different stage the

[53] The cost-effectiveness analysis of some of the principal airlines' security measures is analyzed in section 3.5.

possibility of successful attacks and successful defensive actions and therefore, it identifies a series of mitigation options for each different step, drastically reducing the complexity of the terrorism risk analysis and in consequence, the total expected losses arising from terrorists' attacks (Poole Jr, 2008 and Cha, Ellingwood, Shafieezadeh, 2015).

3.4.3 Principal airlines' security measures implemented after September 11th.

The events of the well-coordinated terrorist attacks of September 11th have underlined a new airlines security threat that must be mitigated and prevented, which is the activity of aircrafts hijacking subsequently used for terrorists' suicide missions (Poole Jr, 2008). Therefore, in order to find a quick solution to this incoming threat, OECD Governments have designated their own single national agency responsible for the country's aviation security. The Transportation Security Administration (TSA) in the United States is the agency in charge of making accurate security policies and regulations for the various entities which are implicated in the airlines-airports business (Poole Jr, 2008). In that occasion, the U.S. Congress has developed a mixed system in which by law, the TSA must conduct the activity of passenger and checked-baggage screening despite it is actually the national airline regulator and policy-maker. On the contrary, the other airport security functions like, access control and perimeter protection, must be provided by airport security companies according to the TSA regulations. In general, the two pre-mentioned activities of screening are provided by private security companies accurately chosen and approved by the TSA agency in order to increase airports efficiency and consequently avoid time consuming (Poole Jr, 2008 and Stewart, Mueller, 2013).

In the aftermath of September 11th, the Transport Security Administration agency has played a vital role in the development of new lines of security for U.S. airlines and airports, and it has collaborated with other European and Canadian agencies sharing their knowledge and main information in a common international network for making aviation security policies more effective and risk-based (Poole Jr, 2008). Consequently, the U.S. TSA agency has developed a new system of "22 Layers of Security" which were eventually designated with the main goal of providing defensive actions and protection for passengers and for the American air transport system (Stewart, Mueller, 2013). A large part of these 22 layers are related to pre-boarding security with specific activities of identification, deterrence and apprehension of terrorists before they physically enter into the aircraft. They are:

1) Intelligence activities;
2) International partnerships;
3) Border and customs protection;
4) Creation of joint international terrorism task force;
5) No-fly list and passenger prescreening with the new system of CAPPS II;
6) Crew vetting, that consists in an accurate examination of aircraft crew members;
7) Visible Intermodal Protection Response (VIPR), which is a new program focused on providing security to any mode of transport in the U.S.;
8) Development of canines' programs, which means the use of trained dogs for explosive detention in the airports;
9) Behavioral detection officers, experts in human behavior;
10) Travel document checker;
11) Checkpoint/Transportation security officers (TSOs);
12) Baggage check operations;
13) Aviation transportation security inspectors;
14) Activities of random employees screening;
15) Bomb appraisal officers.

The other seven remaining security layers are provided during the in-flights phase (Stewart, Mueller, 2013). They are:

16) Passenger resistance to terrorists' hijackings;
17) Training program for flight crews;
18) Hardened cockpit doors in each single carrier;
19) The installation of Physical Secondary Barriers (IPSB) on the airliner;
20) Federal Air Marshal services, which consists in hiring an officer to physical attend the flight to ensure the security;
21) Law enforcement officers;
22) Federal Flight Deck Officers, which allows crew members and pilots to carry guns to defend the flight deck against terrorist attacks.

The last seven level of security can be group in two different categories in addition to the pre-boarding security measures: measures for preventing physical hijacking of the aircraft (passenger resistance, trained flight crew, law enforcement officer and Federal Air Marshal Service) and for avoiding commandeering of the airliner (hardened cockpit door, installed physical secondary barriers and Federal Flight Deck Officers) (Stewart, Mueller, 2013).

All this new security measures for the U.S. airline companies were subject to very long discussions about their effectiveness in the practices of preventing terrorism risk, hence, their benefits and also their costs, in order to understand their real utility for the aviation industry[54] (Stewart, Mueller, 2008).

One of the most important innovation introduced by the TSA post September 11th was the deployment of a more technological airline passenger profiling system called CAPPS II (Computer Assisted Passenger Prescreening System), which has the scope of checking each single passenger, considering commercial and governmental data, in order to assess his security risk (Ghobrial, Irvin, 2004). CAPPS II takes its information from commercial databases which usually contain files about American citizens' businesses, and then it conducts a final check using governmental databases, in order to assign a risk assessment score to every flight passengers with specific colors to identify their riskiness: green for ordinary passengers, yellow for low/medium-risk travelers and red for the most dangerous (high-risk) passengers (Ghobrial, Irvin, 2004). In conclusion, CAPPS II is a system administrated by the U.S. Central Authority which has replaced the old CAPPS I system, which was used and administered by the aviation companies under the federal supervision and regulation. The new system instead, it uses routine information furnished by customers when they make reservations, and so, it is able to provide the passenger profile with his/her own risk level and at the same time it avoids concerns about the data privacy treatment (Ghobrial, Irvin, 2004).

In line with the introduction of the new CAPPS system, airline companies decided to take even more precautions to protect their system and customers privacy against risk of unauthorized access to transaction information and personal data by developing a new Secure Sockets Layer (SSL), especially considering the increase in the number of cyber-attacks after the event of September 11th (Borghi, 2015). In practice, it is a standard security encryption technology which permits the security transmission of sensitive and private data. Moreover, airlines have their own well-functioning cyber risk framework that allows to effectively manage the risk of terrorists' cyber-attacks by minimizing their damages and protecting airlines technological infrastructures (Borghi, 2015 and Ghobrial, Irvin, 2004).

In conclusion, in the aftermath of 9/11, the primary Governments concern was to avoid other tragic events like that one, therefore a radical change in airline security policies was

[54] The cost-benefit analysis of this new security measures is illustrated in section 3.5.

necessary, and it required a more consistent involvement of the U.S. authorities (Poole Jr., 2008). Consequently, the U.S. airline sector has developed a large number of new dynamic and flexible security measures that may provide more effective solution to prevent and mitigate terrorism risk and its effects of the aviation business (Poole Jr., 2008).

3.5 The usefulness of Anti-Terrorism Risk management procedures in the U.S. airline industry

The section is focused on describing the importance of the new risk management techniques applied to the airline sector in the aftermath of 9/11, 2001, by doing an analysis of their usefulness in terms of costs and benefits. To carefully explain the relevance of the airline security measures, the section is divided in three subsections: the first one, underlines the importance of hedging activities in the U.S. airline industry, considering the intrinsic relation between risk management and its role in increasing company value. The second subsection instead, provides the theoretical framework of the cost benefit analysis applied to the innovative U.S. airlines' security measures created in response to the events of September 11th. Finally, the third and last subsection provides a practical analysis on the usefulness of the 22 layers of airports and air carriers' security according to the already explained cost-benefit framework, in order to assess their real cost-effectiveness in hedging against terrorism risk.

3.5.1 The importance of risk management activities in the U.S. airline industry.

The U.S. airline industry offers a useful example for analyzing the key role played by risk management hedging activities in increasing companies' values. In fact, the aviation sector is exposed to several different types of risk, which may affect its operations, customer travel demand, security and corporates' values (Carter, Rogers, Simkins, 2006 and Yilmaz, 2008). The total risk exposure of the industry can be mitigated through the security risk analysis which aims at preventing and controlling incoming risks, especially terrorism risk which has shown a particular high negative impact on the entire air transport system (Yilmaz, 2008).

The numerous implemented deregulation measures applied to the airline sector from the 80s, and in addition, the rising competition with low-cost companies, has drastically change the aviation business, by involving a constant growth in the air travel demand volatility also due

to the numerous conflicts happened in the last thirty years[55], which has led to a situation of political instability between the OECD and the Muslim states (Carter, Rogers, Simkins, 2006). In fact, the airline industry is basically characterized by high fixed costs especially due to the expensive security measures, low profit margins, and it is sensitive to cyclical and seasonal changes. Therefore, in order to survive to this competitive environment, U.S. airline companies must be more efficient, and they must find better solutions for mitigating demand volatility and incoming risks (Yilmaz, 2008).

In addition, the air transportation system is a country's strategic sector because of its key role in providing access to other markets and hence, it implicates more economic activities and commerce with other foreign regions. This appears to be the main reason why the airline industry has experience several radical changes in the last decades (Yilmaz, 2008). It may face with several types of risk (operational, financial, strategic and disaster) but at the same time, it must provide the highest possible standards of security and safety for all its passengers in order to prevent and mitigate business interruptions and decrease in air travel demand (Carter, Rogers, Simkins, 2006).

Therefore, risk management activities are really valuable for airline companies, considering that they provide precious information about how anticipate certain risks and about the complex interaction between different types of risk, including their links and unexpected correlations (either negative or positive) (Yilmaz, 2008). In fact, the periodically launched Airline Risk Management Survey underlines the high importance of risk and security measures implemented by aviation firms, by monitoring their performances and considering cost and benefits of each action. One of the principal results underlined by these surveys is the airline industry risk-based approach, where almost all the airline companies specify the clear need for more and more accurate risk management operations to avoid failures in managing financial, strategic and operational risks which can result in the evaporation of companies' values (Yilmaz, 2008).

In conclusion, according to the risk management surveys, airline ERM measures are determined considering three characteristics: benefits provided to company in terms of enhancing shareholders value and prevention and mitigation of threats, costs of implementation of the measure (such as costs for technical machines or employees training

[55] The most important conflicts that have affected the most the U.S. airline sector because of the rising fear of terrorism, were the Gulf War in 1990-91, the Iraq invasion in 2003-2011 and the war against the Islamic State of Iraq and Syria started in 2015 (Roser, Nadgy Ritchie, 2016).

program), and capacity of integration with other previous security measures and therefore exploiting the opportunity of creating a better integrated risk management approach, which is fundamental to maximize company's efforts in fighting incoming risks (Yilmaz, 2008 and Smithson, Rutter Associates, Simkins, 2005). Thereby, there are evidences which demonstrate the positive correlation between higher airline shareholders value and the use of well-functioning integrated risk management systems, that involve a reduction in the share price sensitivity and demand volatility (Smithson, Rutter Associates, Simkins, 2005).

3.5.2 Theoretical framework of the cost-benefit analysis on the U.S. airlines' new anti-terrorism procedures.

One of the main concerns of the U.S. airline companies is to understand when the applied security and anti-terrorism measures are cost-effective, in terms of benefits for the industry such as real effectiveness in deterring terrorism risk and avoiding reductions in corporate value or business interruption, their enforcement costs and the number of expected lives saved (Stewart, Mueller, 2008). Unfortunately, there are several problems linked with the determination of counter terrorism measures' cost-effectiveness: first, each of this risk management solution is not permanent, and on the contrary, it should be continuously enhanced and adapt to a mutable environment. Second, there is usually few reliable information about what level and types of terrorist activities an airline company may face, and therefore, the anti-terrorism measure cannot be tailored to a specific threat, but instead, it should be flexible enough to adapt to multiple situations. Finally, a lot of information about the security measures' costs is classified and inaccessible due to the involvement of the U.S. Government, and hence, the verification of their real costs is a very hard challenge (Poole Jr, 2008).

A well-structured cost-effectiveness analysis should compare the security marginal costs with the marginal benefits calculated considering the fatalities and property damages avoided. Thereby, the scope of the airlines' risk analysts is to maximize the net benefit, that is benefit minus total costs, using a specific equation (Stewart, Mueller, 2013):

$$Net\ Benefit = p_{attack} \times C_{loss} \times \Delta R - C_{security} \quad (4)$$

where the four factors represent:

1) P_{attack}: it is the probability of successful attacks, which means the likelihood that a successful terroristic attack will happen if no security measures were active;

2) $Closs$: it estimates the total losses sustained in case of a successful attack which are measured in terms of direct impacts, such as fatalities and property damages, and indirect one, like business interruption;
3) ΔR: it expresses the reduction in risk thanks to security measure ability to deter and protect company assets against terrorist attacks;
4) $Csecurity$: it expresses the total costs required for developing the security measures.

Hence, according to equation four, a security measure is cost-effective only when the net benefit is higher than zero (*Net benefit > 0)* (Stewart, Mueller, 2013). Moreover, airline companies consider several risk acceptance criteria which are related to the different types of risks that have to be quantified (social, lives safety, environmental and economic), the quality of available data and the interested parties preferences (Stewart, Mueller, 2013).

One of the main criteria in order to understand the effectiveness of an airline anti-terrorism measure is the expected reduction in the number of fatality, also called the annual cost per life saved (C_{LS}), which is calculated with the following equation:

$$C_{LS} = \frac{C_R}{lives\ saved\ due\ to\ enhanced\ security\ measures} \quad (5)$$

where C_R is the total annual cost spent of on developing security measures (Stewart, Mueller, 2008). Therefore, the two key parameters in order to understand the usefulness of the security measures are the risk reduction due to the introduction of new and more effective security measures (R) and the annual number of lives losses rate (total annual fatalities rate) before the specific security measure is enhanced. In that case, according to the previously analyzed 22 layers of security, airline company shall calculate the effectiveness of both pre-boarding and in-flight security procedures (Stewart, Mueller, 2008).

Hence, considering the first fifteen TSA's layers of security, which are the ones related to pre-boarding anti-terrorism measures, there was a large increase in the amount of extra vigilant intelligence and passport control, and the introduction of new airport checked-baggage and passenger screening and another series of security procedures in result of the events of September 11th (Stewart, Mueller, 2008). The overall effect of the more innovative pre-flight security techniques plus the increased public awareness about terrorism, has resulted in a huge improvement in preventive strategy and policies against terrorism risk which drastically reduce the possibility of a replication of the terroristic attacks of 9/11, 2001. In fact, since that date, no other hijacking has been successfully completed against a

United States airline company, demonstrating the effectiveness of the new layers of pre-boarding security (Stewart, Mueller, 2008).

The last seven layers of security instead, could be subjected to cost-benefit analysis, especially considering the high implementation costs of some of them and the previous consideration about the efficiency of the pre-boarding measures, which can make less determinant some of the in-flight measures (Stewart, Mueller, 2013). They can be divided into four main groups:

1) Crew and passenger resistance, which includes the Federal Flight Deck Officers, the Trained Flight Crew (particularly similar to the first security measures), and passenger resistance, which doesn't involve any kind of costs and it is always the last resort and therefore, it is not considered as a reliable option.
2) Hardened Cockpit Door;
3) Federal Air Marshal Services, which also includes the law enforcement officers;
4) Physical Secondary Barriers (IPSB) on the airliner.

These four groups provide different level of security for the air carriers and therefore, they are the principal subject of the cost-benefit analysis elaborated in the final subsection of this study, in order to give an accurate answer to the U.S. airline research for the most cost-effective anti-terrorism measures.

3.5.3 Practical application of the cost-effectiveness analysis on the new U.S. airlines security measures.

According to the theoretical framework developed in the previous subsection, the study is now focused on providing a practical analysis of the new airports and airlines security measures applied by the U.S. Government and aviation sector, and more specifically, by examining the real effectiveness of the four groups of anti-terrorism techniques previously mentioned.

The first important elements of the analysis are the implementation costs of the four different measures. According to the work of Stewart and Mueller, the Federal Flight Deck Officers and the Trained Flight Crew (which are part of the first group of in-flight security measures) are not very expensive security measures for the for the U.S. airlines (Stewart, Mueller, 2013). The FFDOs program allows pilots and crew members, who voluntarily join the program, to be trained in the use of guns and to possess firearms onboard in order to defend

the carrier and more specifically the flight deck against acts of hijacking. By 2011, nearly 15,000 pilots of U.S. airline companies have joint the program (almost 20% of the total number of pilots). Moreover, if FFDOs are present in a carrier, they are as effective as any other air marshal, but the average cost of an air marshal per flight is around 3,300$, while this measure only costs around $15 per flight. Finally, the official TSA annual budget for FFDOs and crew training program is around $25 million (Stewart, Mueller, 2013).

Instead, the installation of hardened cockpit doors is a security measures required for all domestic and foreign company serving the U.S., and it is very useful for cockpits' protection against small fire arms, fragmentation devices and intrusions (Stewart, Mueller, 2013). According to previous studies, in general, the average costs for each hardened cockpit installation is between $30,000 - $50,000, and hence, the total expenses for a company is around $300 - $500 million over a 10-year period, therefore, around $30 - $50 million dollars each year, also considering the highest cost of fuel consumption due to the heavier installed doors (Stewart, Mueller, 201).

The installed Physical Secondary Barriers is a security measure used during the phases of opening and closing of the cockpit's door, and it has the scope of protecting the flight deck area from trained hijackers. It is a lightweight devise that is easy to deploy or broke and therefore, it cannot provide a very high protection against terrorism risk. It costs around $10,000 - $30,000 for each one, and hence, a total expense for a company between 100-300 million dollars over a 10-year period and around $10 - $30 million each year. We also must consider than not all the commercial carriers have this security measure, but only around 20% of them (Stewart, Mueller, 2013).

The last in-flight security measure is the Federal Air Marshal program, which has an annual budget of more than 950$ million and it involves almost 4000 air marshals in the U.S. Moreover, the program costs almost 250$ million per year in lost revenues for the U.S. airline companies, and it has been calculated that officers fly on no more that 5-10% of the total American flights. This means that the potential presence of air marshal on a carrier and his capacity to deter a terrorist attacks is lower compared to other measures such as the FFDOs. In conclusion, it is the most expensive security measure, with almost 1.2 billion dollars of annual expenses for the U.S. Government and airline companies (Stewart, Mueller, 2013).

Therefore, considering the previous cost measures, the study needs to make some basic assumption in order to develop the cost-benefit analysis:

1) According to the works provided by the scholar Teng T. O, the analysis considers as regulatory safety goal a cost per life saved between $1 – $10 million, which is how much the American society is willing to pay for saving a life without incurring in too much costs (Teng…, 1995). This means than over the 10 million dollars threshold per life saved, the security measure implemented is not cost-effective;
2) In case of absence of reliable security measures, the study considers the possibility of having a disastrous event such as the terroristic attacks of September 11th, every twelve years. Hence, the number of lives saved due to the enhancement of security measures in around 3000 every twelve years, and so, 250 persons saved each year. This is consistent with the results of several scholars works, which have underlined that the number of causalities caused by 9/11 terrorists' activities approximately equals all the terrorist-related deaths during the period between 1988-2000 (Sandler, Enders, 2005);
3) The last assumption concerns equation (4). In fact, the probability of having a successful terroristic attack (P_{attack}) is, by making a simplification for the analysis, equal to the fatality accident rate per 100,000 departures. In 2001, this rate was 0,019 (www.airlines.org), but the analysis considers a possible adjustment due to the fact that the number of departures in 2018 in almost doubled, and therefore, without appropriate security measures, also this rate should be higher. Hence, in a simplified and pessimistic scenario in can be around 0.035. In addition, the total losses sustained in case of a successful attack (C_{loss}), considering both direct and indirect impacts, are equal to the total losses made by the terroristic attacks of 9/11, hence, according to second assumption, it can happen again every twelve years. $P_{attack} = 0.019$; $C_{loss} = \$32$ billion

Having listed the crucial assumptions of the analysis, we have to calculate the risk reduction (ΔR) provided by the pre-boarding and in-flight security measures of the 22 layers of security.

We should start from the 15 levels of pre-boarding security. According to numerous studies, the possibility that a single measure can detect a terrorist activity is particularly low. Therefore, by simplification, the analysis gives a 5% possibility to a pre-boarding measure of preventing a terroristic attack, and hence, considering all the other fourteen security measures, the total risk reduction can be calculated as:

(6) $$\Delta R = (1 - (1 - 0{,}05)^{15} = 0{,}54$$

This result is consistent with other studies that have calculated this risk reduction in a range between 50% and 65% (Stewart, Mueller, 2008 and 2013).

The other four groups of in-flight security measures have different risk reduction measures due to their different characteristics. Considering the pre-boarding result, the on boarding measures can decrease terrorism risk for a maximum of 46%, which is, by making a simplification, equally divided into the four groups.

Δ R (Federal Flight Deck Officers)	$\Delta R = 11.5\% \text{ x } 0{,}2 = 2.3\%$
Δ R (Hardened Cockpit Door)	$\Delta R = 11.5\%$
Δ R (Federal Air Marshal Services)	$\Delta R = 11.5\% \text{ x } 0{,}1 = 1.15\%$
Δ R (Physical Secondary Barriers)	$\Delta R = 11.5\% \text{ x } 0.2 = 2.3\%$

The results of the table clearly show that the risk reduction of the in-flight measures strictly depends on the number of aircrafts in which they are applied. According to the previous information, the FAM active on at maximum only 10% of the total U.S. airline flights, therefore their ability to prevent a threat is linked to their very low presence on carriers. The same statement is valid for the FFDOs (only 20% of pilots and crews are trained) and IPSB (only 20% of the total commercial airplanes have installed secondary barriers). The only measure that is installed to every aircraft by law is the hardened cockpit door.

By assumption, the remaining part of the total risk reduction can be related to the untrained crew and passenger resistance in case of terrorist hijacking, and it cannot be used for calculating the cost per life saved or the net benefit because it doesn't involve any costs for airline companies[56] (Stewart, Mueller, 2013).

According to these risk reduction data, the analysis calculates the annual cost per life saved (C_{LS}) for each different anti-terrorism measures, by using equation (5).

C_{LS} (Federal Flight Deck Officers)	$C_{LS} = \frac{\$25 \text{ million}}{250 * 2.3\%} = \$4.35 \text{ million}$

[56] This analysis is based on assumptions, this means that maybe some of these pre-boarding or in-flight measures may involve more risk reduction capacity than the one predicts by the model. Therefore, by changing this percentage, it is possible to obtain different results.

C_{LS} (Hardened Cockpit Door)	$\mathrm{C_{LS}} = \frac{\$40 \text{ million}}{250 * 11{,}5\%} = \$1.4 \text{ million}$
C_{LS} (Federal Air Marshal Services)	$\mathrm{C_{LS}} = \frac{\$1.2 \text{ billion}}{250 * 1{,}15\%} = \$417{,}4 \text{ million}$
C_{LS} (Physical Secondary Barriers)	$\mathrm{C_{LS}} = \frac{\$20 \text{ million}}{250 * 2.3\%} = \$3.48 \text{ million}$

The final results of the cost per life saved calculation provide support to the general idea that the Federal Air Marshal services is a greatly ineffective security measures, as it was demonstrated by other scholars (Stewart, Mueller, 2013), while all the other three measures are included in the range of the regulatory cost per life saved defined by the first assumption, respecting the maximum threshold of a 10 million dollars expense for saving one life. It also seems that the hardened cockpit door is the most cost-effective security measures, and that the FFDOs is far more useful that FAM program.

At the end, the study calculates the specific net benefit of the outlined anti-terrorism measures, in terms of annual million dollars saved thanks to their application.

Net Benefit (Federal Flight Deck Officers)	N. B. = 0.035 x \$32 billion x 2.3% - \$25 million = \$0.76 million
Net Benefit (Hardened Cockpit Door)	N. B. = 0.035 x \$32 billion x 11.5% - \$40 million =\$88.8 million
Net Benefit (Federal Air Marshal Services)	N. B. = 0.035 x \$32 billion x 1.15% - \$1.2 billion = - \$1.18 billion
Net Benefit (Physical Secondary Barriers)	N. B. = 0.035 x \$32 billion x 2.3% - \$20 million = \$5.76 million

This final calculation provides more evidences in underling the cost-effectiveness in deterring terrorism risk of three out of four in-flight security measures, especially

highlighting the huge net benefit provided by hardening cockpit doors. These results, even if they are based on a series of simplifications and assumption, are consistent with the ones provided by other scholars (Stewart, Mueller, 2008 and 2013), and they finally address the importance of implementing more reliable security measures in order to increase passengers' safety and simultaneously decrease the eventuality of terrorist attacks.

To conclude, it is particularly hard to define the most suitable risk management procedures for hedging against terrorism risk, because of its unpredictable nature and of the extreme dynamic airlines' environment, which means that there will always be multiple efficient solutions that should be tailored to specific situations and hence, they must be flexible enough to adapt to the mutable context (Poole Jr, 2008 and Stewart, Mueller, 2008).

3.6 Conclusion

The extended analysis made in the third and last chapter introduces important results that should be underlined. First, it illustrates the huge economic impact that the terrorist attacks of September 11th, 2001, had on the U.S. airline companies, drastically decreasing their stocks, passengers' travel demand and profits (Drakos, 2004 and Kim, Gu, 2004). This deep analysis definitely shows the inefficiency of past airline risk management techniques to prevent and mitigate a complex threat such as terrorism risk, and therefore, it clearly states the need for more effective security measures for the entire industry. Hence, the second main point of the study is focused on examining the U.S. Government response to 9/11 in terms of the numerous changes involved in the airline risk management sector. The first change was the introduction of the Aviation War Risk Insurance Program, in order to provide insurance coverage to American airlines not anymore provided by the private insurance sector (Elias, Tang, Webel, 2014). The second most important innovation was the development of a new Airline Security Risk Analysis framework, for examining all the plausible threat scenario and therefore, providing the most accurate possible information to U.S. airline companies which facilitates the implementation of the most effective anti-terrorism solutions (Cha, Ellingwood, Shafieezadeh, 2015). The last innovation was the "22 Layers of Security" developed as practical airlines and airports security measures for both phases of pre-boarding and in-flight (Stewart, Mueller, 2008). The last result of the chapter is the demonstration of the positive effect of well-functioning risk management activities on increasing aviation firms' value. Therefore, they are examined more in depth the costs and benefits provided by the innovative 22 airline security measures for American airlines,

highlighting the most cost-effective ones (which is the hardened cockpit door) and least effective one (the Federal Air Marshal Services) (Stewart, Mueller, 2013).

In conclusion, considering the entire analysis, the chapter has a dual scope: to underline the main changes in the U.S. airline risk management practices happened in the aftermath of 9/11 and how much they can affect airline shareholders' value, but also, to explain the inadequacy of the previous aviation security systems in preventing the terrorism threat. Unfortunately, this inadequacy has partially contributed to the tragedy of September 11th.

Conclusion

The thesis is focused on giving a well-detailed analysis of the impacts that terrorism risk has on societies' well-being and companies' economic development, and hence it provides a deep analysis on the evolution of the risk management framework and procedures implemented for preventing terrorism activities. Consequently, because of the huge importance that plays the terrorist attacks of September 11th, the study and the research question is focused on giving a precise and detailed analysis on the most important changes in anti-terrorism policies happened in the U.S. airlines industry (which is the sector that has experienced the highest direct and indirect damages due to this catastrophe) in the aftermath of 9/11.

More specifically, the research question wants to demonstrate the real cost-effectiveness of the new airlines' security measures in terms of net benefit (cost saving due to the implementation of the specific anti-terrorism measure) provided to the airline companies and annual cost per life saved. Furthermore, it is underlined the positive effect that these innovative, reliable and effective measures have in increasing airlines company values.

The first important result of the thesis definitively states, in accordance with several scholars' works, the high difficulties in providing always effective counterterrorism risk measures, due to the dynamic and unpredictable nature of this risk (both in terms of severity of losses and probability of occurrence), which results in a continuous threat for companies and Governments (Woo, 2002 and Amoore, De Goede, 2005). The fact that terrorism risk doesn't meet the insurability criteria defined in chapter one, have made it one of the main issues in the contemporary risk society. Therefore, the study clarifies the need for governmental intervention in order to overcome this issue, and in fact, it describes the functioning and the positive results given by the introduction of both Terrorism Risk Insurance Act (TRIA) in 2002, to stabilize the private insurance market (Michel-Kerjan, 2012), and the expansion of the Aviation War Risk Insurance Program, which guarantees to the U.S. airline companies the requested insurance coverage against terrorism risk, which was not anymore supplied by the commercial insurance market (Borghi, 2015 and Elias, Tang, Webel, 2014).).

The second main result of the study concerns the enormous importance that the activity of modelling terrorism risk plays in defining the most suitable terrorism risk management tools that should be applied by private and public sector (Ezell, Bennett, Von Winterfeldt, Sokolowski, Collins, 2010). The study underlines two main outcomes from this analysis:

first, it is particularly efficient the private-public collaboration between governmental institutions and companies in modelling terrorism risk, especially because it can provide continuous and more reliable flows of information very useful to create consistent risk models and frameworks suited for calculating the terrorism risk exposure (Mazzarella, 2005). The second principal finding in the terrorism risk modelling practice is the importance of having an interdisciplinary approach to provide the best possible terrorism risk estimates. After a careful scrutiny of numerous scholars' works, the thesis states the importance of using a multilateral approach in modelling terrorism risk, by getting the information from different disciplines. In fact, the work underlines the importance of the game theory analysis, with the Attacker-Defender model quite useful in describing a complex phenomenon by using relatively simple equations and assumptions (Major, 2002), then the relevance of the probabilistic risk analysis (PRA), with the three variables Terrorism risk model, which assesses terrorism risk by using only three factors (threat, vulnerabilities and consequences) (Willis, Morral, Kelly, Medby, 2005), and finally the social network analysis based on examining and monitoring terrorists' electronic and social communications, (Risk Management Solutions Report, 2012). At the end, the thesis confirms the interdisciplinary approach adopted by the new Airline Security Risk Analysis Framework in order to obtain fruitful estimations of eventual terroristic activities against the civil aviation (Carter, Rogers, Simkins, 2006).

The final result of the study concerns first, the analysis of the total economic impact of 9/11 on the U.S. air carrier sector (declining travel demand by 30%, huge negative net profits of respectively $13.0 and $11.3 billion in 2001 and 2002, and an average decrease in airline stocks' market prices by 50%…) by providing tables and charts, and finally, the practical analysis of the 22 layers of security introduced by the U.S. airline sector in the aftermath of September 11th. In fact, considering the scholars' debate about the real effectiveness of this measures in preventing terrorism threats, the study gives a personal and experimental analysis about the real usefulness of the airlines security measures.

The analysis is based on assumptions and simplification, and it calculates the net benefit and annual cost per life saved of the in-flight security measures (the more discussed about their usefulness), finding consistent results with other similar works (Stewart, Mueller, 2013). Considering both measures results (C_{LS} and Net Benefit) the most effective one is the hardened cockpit door, while the least effective is the Federal Air Marshal services, which seems too much expensive compared to their real utility in blocking terrorists' attempts of

hijacking or damaging aircrafts. Based on these results, the thesis suggests some changes in the annual expenditure on anti-terrorism procedures, by underling that, in order to save costs and therefore maintain or even increase airlines' economic performances and corporate value, it should be better to invest in the FFDOs program for training a high percentage of crews and pilots, or on other pre-boarding security measures for detecting terrorists.

Clearly these are subjective results and observations, and even if they are in accordance with previous studies (Stewart, Mueller, 2008 and 2013), they cannot be taken as univocal and absolutely correct.

In conclusion, the hundred percent safe flight still remains today a utopia, because of the eventual and new future challenges that may affect the aviation sector. Therefore, it is fundamental, for both domestic and international air carriers, to invest in risk management research in order to provide continues more effective procedures to maximize security and safety for all passengers and to protect airlines business's financial performance from disastrous events and simultaneously foster its growth.

References

Airlines for America Industry Report (2018), "U.S. Airline Industry Review: Allocating Capital to Benefit Customers, Employees and Investors", pp. 1-78.

Amoore L., De Goede M. (2005), "Governance, risk and dataveillance in the war of terror", Crime, Law & Social Chang, Springer, pp. 149-173.

Aradau C., Van Munster R. (2007), "Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future", European Journal of International relations, Vol. 13(1), pp. 89-115.

Baas S., Ramasamy S., Dey de Pryck J., Battista F. (2008), "Disaster risk management systems analysis: a guide book", Food and Agriculture Organization of the United Nations, pp 1-80.

Baldwin D. A. (1997), "The concept of Security", British International Studies Association, vol 23, pp. 5-26.

Beck U. (2002), "The Terrorist Threat: World Risk Society Revisted", Theory, Culture & Society 19(4): 39–55.

Belobaba P., Hernandez K., Jenkins J., Powell R., Swelbar W. (2011), "Productivity Trends in the U.S. Passengers Airline Industry 1978-2010", U.S. Transportation Productivity study, pp. 1-76.

Bin Laden Osama (November 24, 2002), "Letter to America", pp.1-8.

Bjorgo T. (2013), "Strategies for Preventing Terrorism", Palgrave MacMillan, pp. 1-10.

Blomberg S. B., Hess G. (2009), "Estimating the Macroeconomic Consequence of 9/11", Peace Economics, Peace Science and Public Policy, Vol. 15, Issue 2, pp. 1-24.

BMZ Report (June 2015), "Disaster Risk Management: Approach and Contributions of German Development Cooperation", Federal Ministry for Economic Cooperation and Development (BMZ), pp. 1-38.

Borghi L. M. (2015), “Risk Management in the Airline Industry: Financial and Insurance Solutions”, Master Thesis, pp. 60-75.

Bouriaux S., Scott W. L. (2004), “Capital market solutions to terrorism risk coverage: a feasibility study”, Capital Market Solutions to Terrorism Risk Coverage, Vol. 5, No. 4, pp 34-44.

Bruggeman V. (2007), “Capital Market Instruments for Catastrophe Risk Financing”, American Risk and Insurance Association, pp. 1-40.

Carter D. A., Rogers D. A., Simkins B. J. (2006),” Does Hedging affect firm value? Evidence form the US Airline Industry”, Financial Management, pp. 53-86.

Carter D. A., Simkins B. J. (2002), “Do Markets React Rationally? The Effect of the September 11th Tragedy on Airline Stock Returns”, Oklahoma State University, pp. 1-27.

Cha E. J., Ellingwood B. R., Shafieezadeh A., (2015), “A Decision Framework for Managing Risk to Airports from Terrorist Attack”, Risk Analysis, Vol. 35, No. 2, pp. 292-306.

Chaudhuri A., Ghosh S.K. (2016), “Quantitative Modeling of Operational Risk in Finance and Banking Using Possibility Theory”, Springer International Publishing Switzerland, pp. 7-28.

Chavez M. (2007), “Basel II – Pillar II Main guidelines and Practicalities of its implementation”, BMI Paper, pp. 1-24.

Continental Airlines Annual Report (2001), also available on www.annualreports.com, pp. 1-36.

Delta Airlines Annual Report (2001), also available on www.annualreports.com, pp. 1-124.

Dionne G. (2013), “Risk Management; History, Definition and Critique.”, Dionne and Cirrelt, pp 1-22.

Doganis R. (2006), “The Airline Business: Second edition”, Routledge, only specific chapters.

Drakos K. (2004),” Terrorism-induced structural shifts in financial risks: Airline stock in the aftermath of the September 11th terror attacks”, European journal of Political Economy, Vol. 20, pp. 435-446.

Elias B., Tang R., Webel B., (2014),” Aviation War Risk insurance – Background and Options for Congress”, Congressional Research Service, pp. 1-19.

Embrechts P., Furrer H. and Kaufmann R., (2003), “Quantifying regulatory capital for operational risk”, Derivatives Use, Trading & Regulation, 9, pp. 217-33.

Ezell B. C., Bennett S. P., Von Winterfeldt D., Sokolowski, J. and Collins A. J. (2010), “Probabilistic risk analysis and terrorism risk”, Risk Analysis, Vol. 30, No. 4, pp. 575-589.

Franklin J. (2008), “Operational Risk Under Basel II: A Model for Extreme Risk Evaluation”, Banking & Financial Services Policy Report, Vol. 27, No 10, pp 10-16.

Fraser J. R.S., Simkins B. J. (2011), “Enterprise Risk Management: An Introduction and Overview”, John Wiley & Sons, Inc., pp. 1-17.

Galeotti M. (2006), “1986-2006: Vent’anni di prezzi del petrolio”, L’Italia nell’economia internazionale, Rapporto ICE 2005-2006, pp. 69-84.

Ghobrial A., Irvin W. A. (2004),” Combating Air Terrorism: some implications to the Aviation Industry”, Journal of Air Transportation, Vol. 9, No.3, pp. 67-86.

Gold D. (2004), “Economics of Terrorism”, New York: Columbia University Press, pp. 1-22.

Haimes Y. Y. (2004), “On the Definition of Vulnerabilities in Measuring Risks to Infrastructures”, Risk Analysis, Vol. 26, No. 2, pp. 293-297.

Hartwig R. P. (2008), “Terrorism & Enterprise Risk Management: Scenarios & Uncertainty”, Enterprise Risk Management Symposium.

Huntington S. P. (1993), “The Clash of Civilization?”, Foreign Affairs, Vol. 72, No. 3, pp. 22-49.

Institute for economics and Peace Report (2017), “Global Terrorism Index: measuring the impact of terrorism”, pp.1-120.

International Air Transport Association (IATA) Report (2010), “The Impact of September 11th, 2001 on Aviation”, pp. 1-8.

Ito H., Lee D. (2003), “Assessing the Impact of the September 11th Terrorist Attacks on U.S. Airline Demand”, Journal of Economics and Business 57, pp. 75-95.

Ito H., Lee D. (2004), “Comparing the Impact of the September 11th Terrorist Attacks on International Airline Demand”, journal of Economics and Business, pp. 225- 249.

Jorion P. (2012),” Risk Management in the Aftermath of September 11th “, University of California-Irvine, pp. 1-15.

Karolyi G. A., Martell R. (2006), “Terrorism and the Stock Market”, The Ohio State University Working Paper, pp. 1-26.

Kibble D. G. (2002), “The Attacks of 9/11: Evidence of a Clash of Religions”, Parameter-autumn, US Army College, pp. 34-45.

Kim H., Gu Z. (2004), “Impact of the 9/11 terrorist attacks on the return and risk of airline stocks”, Tourism and Hospitality Research, Vol. 5, No. 2, pp. 150-163.

Kousky, C. (2011), “Managing the Risk of Natural Catastrophes: The Role and Functioning of State Insurance Programs”, Review of Environmental Economics and Policy, pp. 153–171.

Kunreuther H. C., Michel-Kerjan E. O. (2007), “Evaluating the effectiveness of terrorism risk financing solutions”, National Bureau of Economic Research Working Paper No. 13359, pp. 6-38.

Kunreuther H. C., Michel-Kerjan E. O. (2017), “The Terrorism Risk Insurance Act (TRIA): unique financing for a unique risk”, University of Pennsylvania, pp. 1-9.

Kydd A. H., Walter B. (2006), “The Strategies of Terrorism”, International Security, Vol. 31, No. 1, pp. 49-79.

Lewis B. (2004), “The Crisis of Islam: Holy War and Unholy Terror”, Random House Incorporated.

Looney R. (2002), "Economic Costs to the United States Stemming from the 9/11 Attacks," Strategic Insights, Vol. 6, No. 1.

Mahmood M. (2002), **“**Terrorism- Definition and Types”, Pakistan Army, pp. 1-29.

Major J. A. (2002), “Advanced Techniques for Modelling Terrorism Risk”, The Journal of Risk Finance*,* vol. 4, pp. 15-24.

Mannik, E. (2009), “Terrorism: its past, present and future prospects”, Tartu University Press, pp.151-171.

Marsh & McLennan Companies Report (2015), “Terrorism Risk Insurance Program Reauthorization Act (TRIPRA)”, pp. 1-32.

Marsh & McLennan Companies Report (2018),” Terrorism Risk Insurance Report”, pp. 1-31.

Mazzarella J. J. (2005), “Terrorism and Multinational Corporations: International Business Deals with the Costs of Geopolitical Conflict”, Major Themes of Economics, pp. 59-72.

Michel-Kerjan M. O. (2012), “TRIA at ten years: The future of the terrorism risk insurance program”, Wharton University of Pennsylvania, pp. 1-12.

Mueller J., Stewart M. G. (2011), “Balancing the Risks, Benefits, and Costs of Homeland Security”, Homeland Security Affairs, Volume 7, pp. 1-27.

OECD (July 16, 2005), “Terrorism risk insurance in OECD countries”, Policy Issues in Insurance, No. 9, chapter one, two, three, seven and eight.

Oprea M. G. (2010), “The Effects of Global Economic Crisis on the air Transport of Passengers in Europe and in Romania”, Vol. 5, No. 1, pp. 52-61.

Poole Jr. R. W. (2008), “Toward Risk-Based Aviation Security Policy”, Discussion paper No. 23, pp. 2-26.

Rhee R. J. (2005), “Terrorism Risk in a Post 9/11 Economy: The convergence of Capital Markets, Insurance, and Government action”, UF Law Scholarship Repository, pp. 437-531.

Riley W. D. (2016), “TRIA and Captives: The Role of Captive Insurance in the Terrorism Risk Insurance Program”, pp. 151-161.

Rippel M., Teply, P. (2010),” Operational Risk – Scenario Analysis “, International Conference on Business, Economics and Tourism Management, pp. 1283-1290.

Risk Management Solutions Report (2012), “Terrorism Risk in the Post 9/11 Era: A 10-Year Retrospective”, pp. 1-32.

Rose A. Z., Blomberg B. S. (2010), “Total Economic Consequences of Terrorists Attacks: Insights from 9/11”, Published Articles & Papers, Vol. 16, Issue 1, pp. 1-12.

Roser M., Nadgy M., Ritchie H. (2016), “Terrorism”, Our World in Data, pp. 1-15.

Sandler T., Enders W. (2005), “The economic impact of terrorist attacks”, Transnational terrorism: an economic analysis, pp 11–34.

Segal S. (2011), “Corporate Value of enterprise Risk Management: the next step in Business management”, Wiley Corporate F&A, chapter 1 and 2.

Simus R. (2016), “The Evolution of terrorism”, Acta Universitatis George Bacovia. Juridica, Vol. 5. Issue 2/2016, pp 1-6.

Smithson C., Rutter Associates, Simkins B. J. (2005), “Does Risk Management Add Value? A survey of the evidence”, Oklahoma State University, Vol. 17, No. 3, pp. 8-16.

Stewart M. G., Mueller J. (2008), “A risk and cost-benefit assessment of United States aviation security measures”, Springer, Vol. 1, Issue 3, pp. 143–159.

Stewart M. G., Mueller J. (2013), “Terrorism Risks and Cost-Benefit Analysis of Aviation Security”, Risk Analysis, pp. 893-908.

Teng T. O., Adams M. E., Pliskin J. S., Safran D. G., Siegel J. E., Weinstein M. C., Graham J. D. (1995), “Five-Hundred Life-Saving Interventions and their Cost-Effectiveness”, Risk Analysis, Vol. 5, No. 3, pp. 369-390.

Thomas J. E. (2003), “Exclusion of Terrorist-Related Harms from Insurance Coverage: Do the Costs Justify the Benefits?”, Indiana Law Review, Vol 36, pp. 1-27.

UNISDR Report (2013), “Small Businesses: Impact of Disasters and Building Resilience”, Background Paper prepared for the Global Assessment Report on Disaster Risk Reduction, pp. 1-76.

United States Government Accountability Office (2005), “Catastrophe Risk: U.S. and European Approaches to Insure Natural Catastrophe and Terrorism Risks”, pp. 1-80.

Vickers E. W. (2015), “The future of managing Terrorism Risk: industry challenges & opportunities”, Honor Thesis, pp. 1-27.

Virgo J. M. (December 2001), “Economic Impact of the Terrorist Attacks of September 11, 2001.” Atlantic Economy Journal, No. 4, pp. 353-357.

Webel B. (2013), “Terrorism Risk Insurance: Issue Analysis and Overview of Current Program”, Congressional research service, pp. 1-15.

Weiss D., Maher M. W. (2008), “Operational hedging against adverse circumstances”, Journal of Operations Management, pp. 362-373.

Willis H. H., Al-Shahery O. (2014), “The National Security Perspectives on Terrorism Risk Insurance in the United States”, RAND Corporation, pp. 1-26.

Willis H. H., Morral A. R., Kelly T. K., Medby J.J. (2005), “Estimating Terrorism Risk”, Center for terrorism risk management polic*y,* pp. 1-66.

Wolfendale J. (2006), “Terrorism, Security, and the Threat of Counterterrorism”, Studies in Conflict & Terrorism, pp. 753-770.

Woo G. (2002),"Quantitative Terrorism Risk Assessment", The Journal of Risk Finance, Vol. 4 Iss 1, pp. 7 – 14.

Yilmaz A. K. (2008), “Importance of the Enterprise Risk Management Practice for Airline Management: ANP- based Approach”, International Journal of Business and Management, Vol. 3, No. 5, pp. 138-146.

Website List

www.bbc.co.uk

www.nytimes.com

www.airlines.org

Bloomberg

SUMMARY

The thesis is focused on providing an extended analysis on terrorism risk and the evolution of the risk management techniques applied by U.S. airline companies after the terroristic attacks of September 11th, 2001. This event was a turning point in the worldwide history, because it was the greatest terroristic attack ever happened, which has caused 2996 casualties and more than 32 billion dollars of property damages, and moreover, it has dramatically worsened the OECD countries and Muslim states relationships, since from that day the "War on Terror" has begun. The study highlights the inadequacy of the anti-terrorism measures implemented by the U.S. aviation sector before 9/11.

Therefore, the first goal of the work is to introduce and analyze the numerous changes that have affected the insurance industry and the risk management sector after September 11th. These changes are illustrated in terms of new security measures, new terrorism risk models in order to enhance the capability of preventing and mitigating other terrorist attacks, new insurance and reinsurance policies developed to safeguard the private insurance market and finally, innovative risk financing alternatives to hedge against terrorism risk. Moreover, the study underlines the crucial role plays by Governments in restoring the citizens well-being and economic development by promoting a fruitful collaboration between national institutions and private companies.

The second main point of the work is the analysis of the specific effects of the terrorist attacks of September 11th on the U.S. airline industry, by providing tables and charts in which are resumed the principle effects of the event and, the principal changes in security policies applied by U.S. aviation enterprises. Furthermore, the work provides a cost-benefit analysis of the new airline procedures in order to define which are the most cost-effective in hedging against terrorism risk.

Finally, the study highlights the relevance of risk management techniques in improving companies' value, thanks to their capacity to predict and mitigate incoming threats and risk and therefore, to provide both more reliable economic and financial figures and lower uncertainty level for stakeholders.

According to the previous considerations, the first chapter of the thesis presents the analysis and definition of terrorism risk, and it basically underlines the origins of this new emerging threat and the several difficulties encountered in creating hedging instruments against terrorism risk.

To provide a well-structured analysis, an historical digression has been done about the evolution of risk management techniques, especially focusing the examination on operational risks and disaster risks (the latter risks are a sub-category of the operational risks and they also include terrorism risk). The implementation of the new Enterprise Risk Management (ERM) is viewed as the natural evolution of the traditional risk management, and it has tried to solve all the precedent challenges providing a better risk-return decision making process. The Enterprise Risk Management approach, considers all the risk areas as a part of a unique, integrated and enterprise-wide system, and simultaneously, it provides a wide variety of techniques for analyzing and managing risks in a more holistic way with a double extent of assimilating the new risk approach in the corporate culture and enhancing company value. Finally, due to the new ERM model, the analysis of operational risks was completely reviewed and implemented for having a better response to this wide variety of risks in continuous expansion.

As previously said, one type of operational risks are the disaster risks, which are defined as all the unexpected natural or man-made disasters, divided in several types, such as weather related (hurricanes), health related (pandemic), accidental (fire), general act of destruction (war, terrorism, rioting) or specific act of distraction (sabotage), and environmental damages. Therefore, disasters may seriously affect citizens and communities destroying temporarily and sometimes even for many years, the livelihood security of their members. Hence, in order to better control natural and man-made hazards, a precise Disaster Risk Management framework was implemented, with the aim of reducing the vulnerability of communities to extreme disaster events. It can be viewed as a complex and continuous process of planning and implementing adapting strategies and methodologies that involves physical and non-physical measures for the analysis and mitigation of disaster risks with the scope of reducing hazards and vulnerabilities and reinforcing adaptation capacities of individuals and communities.

After having analyzed disaster risk, the study concentrates its attention on terrorism risk, as it is a specific man-made disaster. It firstly states the several difficulties encountered in providing a univocal definition of the word terrorism. In fact, having a universal definition is crucial for coordinating the international collaboration between countries and having a quick response to terroristic attacks. In addition, without a clear definition of what terrorism is, any duties or responsibilities can be charged against countries that support terroristic groups or they are involved in state terrorism, nor any actions can be taken to fight terroristic

organization and their allies. Secondly, the thesis lists the different goals and strategies implemented by terroristic organizations, thanks to the numerous studies made in the last decades, which provide a more reliable knowledge on terrorism and its forms that can assist Governments and international institutions in preventing this complex and dynamic phenomenon. They have been identified ten different types of terrorism: state terrorism, state sponsored terrorism, nationalist terrorism, religious terrorism, left wing terrorism, right wing terrorism, anarchist terrorism, suicide terrorism, cyber terrorism and nuclear and biological terrorism.

Moreover, international entities have also deeply analyzed the main strategies that terrorists applied to achieve their goals. Because usually terrorist organizations are too weak to impose their will directly, they use specific strategies based on persuading target audience's perception to accomplish their wishes by altering their believes, giving a sense of legitimacy to their actions, imposing a degree of commitment to their cause, and finally, they established a good and transparent communication of their intents with people, with reasonable and precise goals to reach. Therefore, the thesis results state the five different implemented terrorists' strategies used for reaching their scopes: attrition, intimidation, provocation, spoiling and outbidding. In addition, literature has also defined the five principal terroristic goals: regime change, territorial change, policy change, social control and status quo maintenance. At the end, it is introduced the Global Terrorism Index (GTI), which is a specific index that considers direct and indirect impact of terroristic actions in 162 states in terms of property damages, number of killed persons, number of injuries and psychological effects that terrorism has on population. It is particularly useful because it is used to compose an accurate score in order to rank every nation according to terrorist organizations' activities on its territory.

After the extended examination on terrorism and its basic characteristics (definition, forms, strategies and goals of terroristic organization, and the GTI), the thesis focuses its attention on terrorism risk and its relationships with the modern society, also called risk society. According to Beck's works, there are at least three different and unquantifiable threats in the world risk society: ecological problems, recurring global financial crises and the rising of terrorism organizations. Terrorism is completely different from the two previous ones because it involves intentional bad actions with the aim of producing fear and socio-economic crises and simultaneously damaging people security. The concept of security is today one of the most important things that the world risk society must provide to their

citizens. Therefore, the advent of the new risk society has led to the arise of a precautionary practice which has in turn guided to new configurations of risk management that mandatorily required to avoid at all costs possible disastrous prospectus of the future. Unfortunately, at the same time, in the modern society, risk is a very difficult factor to predict, either because a multitude of risks flourish continuously, either because they are usually inter-correlated and difficult to analyzed in isolation. Therefore, taking precautions against terrorism and other not easily calculable risks has become one of the main relevant activities in the risk society.

Given this strict relationship between terrorism risk and modern society, Governments became aware of the drastically underestimation they have made on terrorism and the high exposition of their risk portfolio to terrorism risk effects. Therefore, the conventional methods of insurability of terrorism risk were put into question, mainly because of their inability to hedge against such disastrous event like the terroristic attacks of September 11th. Terrorism risk seems to be, for five different reasons, one of the most difficult risk to hedge. In fact, there are no reliable historical data that can be used for future predictions; it has a very dynamic and adaptable nature; there is few available information that can be useful for the insurer; governmental domestic and foreign policies influence terrorism risk; interdependent security may cause losses if they are not implemented with the same level of efficiency. All these challenges create a consistent risk ambiguity which make terrorism arduous to hedge compared to other disaster event.

Moreover, the thesis states that the four insurability criteria (assess ability, randomness, economic insurability and mutuality) are not exactly matched by terrorism risk. Hence, for all these reasons, terrorism risk constitutes a critical challenge for the insurance industry, and therefore, it requires the intervention of governmental authorities, which have implemented several changes in order to improve their risk management measures' responsiveness to the threat of terrorism. Furthermore, insurers and Governments have considered a terrorism risk sociologist approach, which takes into consideration human factors as intelligence, network of relationships, social interactions among terrorists, and the hierarchical structure of terroristic groups.

After these considerations about terrorism risk, it is presented an extend analysis of conventional and unconventional methods for hedging against terrorism risk and also explains the importance of modelling terrorism risk.

Starting with the conventional insurance and reinsurance policies, in the aftermath of the terroristic attack of September 11th, insurance industry and Governments have faced a significant change in the treatment of terrorism risk. In fact, in that period, insurers (especially private American insurers), have found themselves with a very high amount of not hedged terrorism risk exposure in their portfolios and with very limited possibilities of reinsurance in order to reduce and prevent probable future losses due to other terroristic attacks. It was clear that the insurance industry could not support alone the threat of terrorism, and so, political pressure forced Governments to act and implement anti-terroristic actions and new insurance program to solve this dramatic situation.

The most important Government intervention in order to control and mitigate terrorism risk was the insurance program developed by the U.S. in 2002. In the U.S., the insurance market was quite unprepared to a similar catastrophe and in few months terrorism risk insurance became unavailable or extremely expensive because a large number of state regulators decided, concerned about the pressing insurers request, to exclude terrorism risks from commercial policies. Therefore, to respond to the fear of economic damage due to the absence of commercially available coverage, in November 2002, the U.S.A Congress intervened by enacting the Terrorism Risk Insurance Act (TRIA), that provided a federal backstop for insurance claims linked to terrorism activities, created as a provisional measure until the insurance industry has developed an adequate solution for hedging against terrorism risk. Under the TRIA program, Governments would provide partial coverage for damages created by terrorism activities considering different thresholds of losses.

The Terrorism Risk Insurance Act had three main goals: to create a provisional federal program base on a private-public partnership in order to compensate the insured for terrorism losses and to stabilize the insurance market, to protect customers providing available insurance policies against terrorism risk, and finally, to preserve the state regulation of insurance. After its introduction, the premiums of terrorism insurances where substantially reduced and stabilized and hence, because of its usefulness, it was two times re-extended by the U.S. Congress until 2020.

In this specific occasion, national Governments play a crucial role in preventing and managing terrorism risks. Hence, the thesis explains the main forms of Government intervention (primary insurer, reinsurer of last resort and lender of last resort) and their limits and drawbacks (such as operational rigidities and bureaucratic excesses or the long-term limitation on private insurance industry maneuvers).

After the conventional insurance policies, the study presents the two main forms of unconventional tools for preventing terrorism risk: alternative risk management solutions and alternative risk transfer instruments.

The first group, alternative risk financing instruments have the specific scope of offering high availability of funding in order to accelerate the economic and social recovery of a community who has suffered from terrorism losses. They also have the purpose of guarantee access to future financing opportunities under predetermined conditions.

The second group instead, the unconventional risk transfer instruments, aim at shifting all or part of the financial weight associated with terrorism risk to one party to another. Insurance companies created these alternative transfer instruments for having protection against natural catastrophes such as hurricanes, windstorms, floods and earthquakes. They also have specific characteristics (provide tailor made solutions, multi-dimensional coverage, used derivative instruments…) and the most important alternative risk transfer tool is the terrorism bond, originated from the previous catastrophe bond.

At the end, both alternative risk financing and alternative risk transfer, seems to be useful in the practice of coverage of terrorism risk, but they absolutely required the assistance of modelling firms that must develop reliable and efficient terrorism risk models for preventing and understanding frequency and severity of the events.

Thereby, the thesis empathizes the importance of modelling terrorism risk in order to have more available and reliable information for preventing terroristic attacks and for better implementing both conventional and unconventional risk management measures. In fact, in the aftermath of September 11th, terrorism risk modelling methods have been continuously updated and companies have created several new analytical tools for better measuring terrorism risk.

The innovative terrorism risk model techniques take into consideration several different disciplines in order to apply a multilateral approach in measuring terrorism risk for obtaining better risk previsions. According to this interdisciplinary approach, the thesis presents three principal models used for terrorism risk calculations, each one based on different disciplines:

1) The Attacker-Defender model, which is a simplified model based on game theory assumptions, that explains the possible choices that terrorists (attacker) and government or insurance industries (defender) possess for implementing their strategies. It is particularly important for its ability to describe a very complex phenomenon with a simple equation and a relatively small number of assumptions;

2) The three variables Terrorism Risk model, based on the probabilistic risk analysis (PRA), which expresses terrorism risk as a function of three different variable: threat, vulnerability and consequences. Hence, risk is defined as "the expected consequences over some period of time to a defined set of targets, resulting from a defined set of threats;
3) Terrorism risk model based on the Social Network Analysis, which analyses and monitors the activities of terrorists' electronic communications. In fact, terrorists' communication and social network activities can be intercepted by intelligence and security services, and their data may be used to interdict terrorists' plans.

To summarize these final considerations, developing more effective and reliable terrorism risk measures (both conventional and unconventional) and models, have particular relevance not only for the wellness of citizens and for the security of the community, but also for the economic actives of all multinational and national firms. In fact, global terrorism has very high costs for multinational enterprises and cannot simply be ignored; on the contrary it must require the development of reliable anti-terrorism measures. There are an immense range of benefits both for multinational firms and governments in hedging against terrorism risk, which far outweigh the costs. Therefore, the primary benefits of models and policies aimed at hedging terrorism risk should be the reduction of costs and the stabilization of international business for companies.

Once it has been explained the importance of hedging against terrorism risk and all the major changes happened in the risk management sector in aftermath of September 11th, the study provides an extended analysis of the main consequences and specific changes happened in the U.S airline industry after the terroristic attacks of September 11th, which was the most damaged sector and therefore, it required a more radical federal intervention for overcoming the situation of crisis.

The last chapter describes the historical background of the terrorist attacks of September 11th, in order to underline the principal reasons that may have led to the terrorist attacks, such as the Military intervention of OECD countries in the Middle East, the advent of Globalization, which eventually spread western culture and mindset in the Islamic states and the continuous clash of religions between Islamists and Christians due to a substantial difference in values and believes. All these motives, allowed the development of extremist Islamic movements whose final aim was to hardly strike Western countries in order to

demonstrate their power and free their people from Western states' compulsion and corrupted values.

Consequently, they are presented all the global consequences of 9/11 terrorists attacks. On that day, 2996 persons died, over 6000 were injured in the four different attacks, and it was estimated a total property damage for more than 32,5 billion dollars. The tragic event of 9/11 has involved negative economic consequences for both the U.S. and the worldwide economy, and therefore, the year 2001 was a very difficult and turbulent year characterized by numerous enterprise scandals, the headwinds of a recession and in addition, the tragedy of September 11th. This event has significantly affected the global economy, spreading fear of travelling around the world and consequently, directly impacting several sectors, such as airlines, travel services and insurance. Due to the decrease in the air traffic in the months after the incident, especially in the last twenty days of September when the traffic plummeted by 34%, the airline sector has experienced huge economic losses. By time, the U.S Government and the Federal Reserve were able to mitigate the negative consequences of September 11th, restoring the previous levels of wellbeing and safety in the American society.

After the general considerations about the negative impact of September 11th, the analysis is focused on providing more specific consequences on the U.S. airline industry. Unfortunately, the American airline industry was already experiencing a difficult situation when the disaster happened, where many airline corporations have declared bankruptcy and many more have reported net losses in billion dollars in the last year. In fact, before the events of 9/11, the U.S. airline firms were already experiencing a decrease in company profits, passing from $4,686 millions in 1999 to $2,237 millions in 2000 until the huge loss of more than 8 billion dollars of 2001. The principal reasons that started this negative trend, was the increase in the jet fuel prices, due to the precedent Gulf War and during the years of the Asian crisis from 1998-2002. Moreover, there was a general increase also in airlines labor costs and non-labor costs, which has involved the rise of the total operating expenses of U.S. airlines, consequently reducing their economic performance.

Finally, the approval of the U.S. Congress Deregulation Act passed in 1978, has completely changed the competition rules of the aviation sector and seriously affected the U.S. airlines economic performance. Furthermore, the deregulation pressure supported by the U.S. Government in the international travel between U.S. and other countries, especially with European states, has led to creation and consequently expansion of low-costs companies

(LCCs), which proposed different business models and pricing strategies compared to the more established national carriers and this has implied a strong increase in the international airlines' competition.

The terrorist attack of September 11th has involved total losses for more than $142 billion in the period between 2001-2010 for the U.S. domestic aviation market. Therefore, the study is focused on providing an analysis of the total economic impact of September 11th on the American airline industry by examining a sample composed by some of the most important U.S. air carriers (American Airlines, Southwest Airlines, Frontier Airlines, United Airlines, Delta airlines and Continental Airlines) and non-U.S. airlines (Air New Zealand, Air France, Alitalia, British Airways and Qantas Airlines). The work considers two important variables: airlines' revenues, which are strictly correlated with the number of passenger (the only source of revenues for commercial airlines) and therefore, a decrease in company's revenues can be only related to a decrease in the number of passenger and/or a cost increase, and the changes in the stocks' market prices.

The work demonstrates a clear decrease in revenues due to the mistrust of precedent customers in the airlines' security measures which has led to the spread of the fear of flying, and hence, their decision to use alternative means of transports especially for short distances, or to pick the flight services handled by other airline companies. Moreover, it also underlines that the average of the U.S. airlines' price devaluation on the first day of trading after 9/11 was around 50%, consistent with literature's results.

Hence, considering these circumstances, it is highlighted the airlines' need to introduce new practical security measures and insurance hedging techniques in order to avoid other catastrophes such the 9/11 and to exit from the years of crisis.

The first important change was the expansion of the federal Aviation War Risk Insurance Program in order to guarantee to the American airlines the requested insurance coverage which was not anymore supplied by the commercial insurance market. With this intervention, the commercial insurance market has reached a phase of stabilization and a large number of airlines could again purchase a war risk coverage from private insurers.

The second fundamental change was the application of a new risk management framework for U.S. aviation industry was developed after the events of 9/11, called Security Risk Analysis framework. It is based on five different steps: Scenario Identification, Consequence and Criticality Assessment, Security Vulnerability Assessment, Threat Likelihood Assessment and Life-cycle Cost Assessment. It provides a better estimation of key risks

contributors and the simultaneous identification of the most relevant parameters which increase the level of uncertainty for an air carrier.

Finally, the Transportation Security Administration (TSA) of the United States has developed a new system of 22 Layers of Security for airlines and airports, which were designated with the main goal of providing defensive actions and protection for passengers and for the American air transport system. They are divided into two groups:

1) Pre-boarding security measures (15 out of 22), with specific activities of identification, deterrence and apprehension of terrorists before they physically enter into the aircraft;
2) In-flight security measures (7 out of 22), implemented during a normal flight in order to avoid hijacking.

These measures (especially the in-flight securities) are subject to the cost-effectiveness analysis in the last part of the study, in order to provide their real level of usefulness in preventing terrorism risk.

Moreover, the TSA introduced a more technological airline passenger profiling system called CAPPS II (Computer Assisted Passenger Prescreening System) in the aftermath of September 11th, 2001.

The last part of the thesis is focused on describing the importance of the new risk management techniques applied to the U.S. airline sector in the aftermath of 9/11, 2001, by creating an analysis of their usefulness in terms of costs and benefits. Therefore, it is introduced the theoretical framework of the cost-benefit analysis, by providing the main assumptions and formulas for calculating the Net Benefit and the annual Cost per Life Saved, the two most important indicators of security measures effectiveness.

(1) $$Net\ Benefit = pattack \times Closs \times \Delta R - Csecurity$$

(2) $$C_{LS} = \frac{C_R}{lives\ saved\ due\ to\ enhanced\ security\ measures}$$

The study basically analyses the in-flight security measures (which are the most discussed by literature) considering their different implementation costs, and they are grouped into four types:

1) Crew and passenger resistance, which includes the Federal Flight Deck Officers, the Trained Flight Crew;
2) Hardened Cockpit Door;

3) Federal Air Marshal Services, which also includes the law enforcement officers;
4) Physical Secondary Barriers (IPSB) on the airliner.

These four groups provide different level of security for the air carriers and therefore, they are the principal subject of the cost-benefit analysis elaborated in the final subsection of this study, in order to give an accurate answer to the U.S. airline research for the most cost-effective anti-terrorism measures.

In order to provide consistent results, the empirical study is based on a series of assumptions and simplification in accordance with the consulted literature:

1) The analysis considers as regulatory safety goal, a cost per life saved between $1 – $10 million, which is how much the American society is willing to pay for saving a life without incurring in too much costs;
2) In case of absence of reliable security measures, the study considers the possibility of having a disastrous event such as the terroristic attacks of September 11th, every twelve years (with the same number of fatalities);
3) The probability of having a successful terroristic attack (P_{attack}) is, by making a simplification for the analysis, equal to the fatality accident rate per 100,000 departures, and moreover, the total losses sustained in case of a successful attack (C_{loss}) are equal to the total losses made by the terroristic attacks of 9/11.

According to these assumptions, the analysis first calculates the level of risk reduction for both pre-boarding measures and for each one of the four groups of in-flight measures. Subsequently, the study calculates the annual Cost per Life Saved and the Net Benefit provided by the four on-boarding measures.

Finally, the analysis demonstrates the effectiveness of this measures in hedging against terrorisms risk. The results clearly show the most cost-effective security measure, which is the hardened cockpit door, and the least effective one, the Federal Air Marshal Services. More in general, it is underlined that, having more reliable and efficient anti-terrorism measures, is fundamental for increasing aviation firms' value, and hence, there is a positive relationship between well-functioning risk management activities and positive economic performances.

In conclusion, even if the hundred percent safe flight still remains today a utopia, it is fundamental, for both domestic and international air carriers, to invest in risk management research in order to provide more effective procedures to maximize security and safety for

all passengers and to protect airlines business's financial performance from disastrous events and simultaneously foster its growth.