The “scourge” of terrorism inscribes into the logic of illegal violence, though one must accept there is a lot of subtypes which merits to be discussed. Cyber-terrorism not only seems to be an emergent form of terrorism that escapes to the definition of illegal violence but the paradox lies in the fact sometimes the nation-state, which was originally designed to protect citizens, violates the constitutional rights in the name of security. Cyber-espionage, cyber-terrorism and cyber-crime are concepts inextricably intertwined. Snowden’s case reveals two important assumptions. On one hand, the discourse of surveillance appeals to what Foucault denominated as “the economy of discipline”, which means that any perceived risks allude to a much deeper and preexisting economic matrix (Foucault, 2003). On another, while states devote considerable time and efforts struggling against terrorism to make from this society a better place, important constitutional rights are being vulnerated (Korstanje, 2015). In addition, unlike classic terrorism, cyber-terrorism operates from a virtual landscape which is very hard to grasp.

In this ever-changing and globalized World, the steps of nations to prevent future terrorist attacks are at snail pace. This does not mean nation-states are inefficient to keep the social order, but terrorism operates in the dark side of uncertainty. Since nobody knows where the next blow will take place, specialists have many limitations to forecast the next attack. The forces of securities are clearly identified, but not terrorists. This point opens the doors to a clear sentiment of paranoia and panic, which are the main goals of terrorism. As Luke Howie (2010) puts it, terrorists do not want to kill a lot of peoples, they like a lot of people watching what they have accomplished. This suggests that terrorists and media are two sides of the same coin. The challenge for democratic societies consists in developed democratic solutions to prevent undemocratic expression of violence. In doing so, they should not to lose the sight that terrorism and cyber-terrorism shares the same commonality respecting to trust. Both act to undermine the necessary trust in order for lay people to legitimate their loyalties to authorities.
THE CHALLENGE

Let’s explain first my recent traumatic experience with a Trojan virus which introduced in my personal Computer corrupted all existent Word files. This begs a more than interesting point, how does it happen?

Originally, I received an email from a colleague at Palermo University saying “please review the attached file for me”. Confident his email was genuine; I double clicked the document opening the doors to a virus that affected many of documents. Doubtless it started a real nightmare. Since my recent backup copy dates back January, not only I lost a great part of my academic production from March on, but also it expressed a frightening sensation since my private life was somehow Vulnerated.

The efficacy of virus depends upon its capacity to contaminate networks taking advance of social ties among members. I would never accept a spam from an anonymous source unless by a colleague. As this backdrop, in fact, I did not lose nothing, my house was there, my Pc was there, my family had health. Then, though I lost everything, I have lost nothing. This point suggests two important things. First and foremost, we work on a society which is based in abstract information, produced and disseminated through a virtual platform. What lies there is very important for capitalist societies, though it cannot be physically touched nor grasped. As society of information, words are exchangeable commodities which delineate the borders between reality and virtuality. A person may lose all its savings in a day when a hacker empties the bank account. This intersection of reality with virtuality seems to be one of aspects that facilitated the expansion of capitalism, which are not shared by other human organization as hunter-gatherers, or other ancient civilization. As Naisbitt puts it, the means of production, as well as the profits, tend to be abstracted over the recent decades (Naisbitt, 1984). Secondly, specialists have unclear the limits between cyber-terrorism and terrorism (Verton & Brownlow, 2003). In this respect, some conceptual differences should be in depth discussed.

While terrorists look to cause political instability by the administration of fear, in which case, they serve to adjoin to spectorship through the media (Eid, 2014; Howie, 2010; Korstanje, 2015, 2016), cyber terrorists work in secrecy, never vindicating their acts of vandalism unless if necessary. No less true is that terrorists are in quest of producing a culture of witnessing to produce a symbolic blow, whereas cyber-terrorists have diffuse goals. Some of them seek criminal acts, while others introduce harms to extract vital information from government agencies. Likely, I felt the same terror once I have been confirmed by experts the whole portion of my word files were encrypted or deleted, than audience while bombing or shooting. At the same time, thoughts struck me that there were higher probabilities an attack of this calibre may be very well repeated, waking up a sentiment of anxiety inside me. I bought some updated antivirus software and ensured the necessary back-up
copies. Of course, this thesis suggests that surprise factor is the secondary point in common between terrorism and cyber-attacks. As stated, it is important to discuss, with invited academics, cyber-terrorism as a much wider theme which alternates contrasting position towards the formation of an all-encompassing model.

THE SEARCH FOR SOLUTION

Though at some extent, terrorism and cyber-terrorism are problems which remain unresolved up to date, the examples of FARC in Colombia, ETA in Spain and other classic cells as IRA in United Kingdom evince there are many possibilities to bring this issue to a safer port. Professor James Piazza argues that one of the aspects that determine the radicalization of some groups depends how their original claims are addressed by state. Whenever the group is pressed to operate from clandestinity or has marginal participation in the democratic system, there are higher likelihoods to adopt violent tactics that may very well leads to terrorism (Piazza, 2008). Other studies as McCauley and Moskalenko (2008) and Moskalenko and McCauley (2011) suggest that the radicalization of terrorists depend on the articulation of different stages that oscillate from self-esteem to be accepted by peers, to physical isolation in small groups where opposition to leaders are limited. The various facet of radicalization not only are emotionally in consonant with candidate´s inner-life, but also takes advantage of those people who had a bad image of society and world to instill a radicalized hate. In this vein, Korstanje (2015) has developed an interesting model to understand that the core of terrorism has nothing to do with violence nor religion, but it associates to extortion. One of the problems policy makers, authorities and governments are facing today respecting to terrorism depend upon they do not understand to what they struggle. Terrorism should be defined as a dialectics of hate, which is triggered by a group of insurgents and state. Since state never manages accurate information on where the next attack will take room, sometimes torture surfaces. The oxygen of terrorism and cyber-terrorism not only is previously determined by the generated fear, but as Mahmoud Eid observed, the leading role played by media covering terrorism-related news. Using the fear of citizenry to extortionate a state that somehow is unable, unfit or indifferent to terrorist´s claims is a key factor that explains “the individual radicalization”. These groups recruit youth people, who are seduced by peers or relatives to balance their frustrations feeling they are part of something exceptional, important, and historic. The best form to struggle against terrorism combines further education, with less appetite for witnessing news containing cruelty, violence and death. As civilization, our own prone to consuming “the other death” is conducive to the rise and expansion of terrorism. While we are disgusting (or shocked) for what recently happened in Paris, Nice and other important capitals, we do not let stopping to watch!
ORGANIZATION OF THE BOOK

The present book was oriented to students, scholars, practitioners concerned by the fields of cyber-security in a moment where information is vital for strategic success decision making process. I will explain why cyber-terrorism cannot be dissociated from terrorism in spite of their differences. For those readers who want to open the pages of this book, I should stress, it is intended to re-discover new horizons of research for the decades to come.

As the previous argument given, it is noteworthy that this book is organized in three sections, which deal with different aspects of cyber-terrorism, risk perception, democracy and civil discontents. Over recent decades, specialists focused on the global nature of capitalism and its derived risks. The fact is that in a world where travels, news and information go faster than other periods, the effects of terrorism are much worse in urban cities than other rural zones.

Chapter 1 provides with a fresh view to implement in models that are oriented to prevent web parameter tampering attacks. This model checks parameters with stored database server for validation, at the time it validates resulted outcomes.

Chapter 2 thematises on the possibility to monitor cyber-attacks and risks by means of the implementation of a cyber-security centre. Not only cyber-security represents a chief factor to enhance the well-being of nations, but also is vital to struggle against terrorism. While a centre is created two external requirements should be met, authorative and normative, which are adjoined to internal quests as marketing organization and sales. All operational consideration to implement an efficient centre for control and surveillance in cyber-spaces is adamantly discussed in this recommending chapter.

Chapter 3 reviews the necessary big data to predict social and individual behaviour in terrorism hot-spot or conflict-driven zones. By the exploration of different key variables as age, gender composition, nationality, origin, social status, this model hints interesting results which would help to boost security in zones whipped by “the scourge of terrorism”.

Chapter 4 brings into question to what extent existing infrastructure plays a leading role in the configuration of security. Besides focusing on financial and electric power as potentially risks for next cyber-attacks, he holds the thesis that transport infrastructure should be analysed alternating quantitative and qualitative methods instead. A lot of cyber-attacks to transportation sectors have taken place over the recent years and of course this offers a fertile ground to understand the intersection of terrorism and mobility.
Chapter 5 introduces a short debate respecting to how protestant Reform developed a climate of distrust which is conducive not only to terrorism but risk perception. Theoretically speaking while technology would be used to make of this world a safer place, the needs to anticipate future events a discourse which is expressed under the doctrine of precautionary principle, to avoid threats and risks.

Chapter 6 calls the attention to the atmosphere of distrust Governments and their agencies are facing today. Part of this derives from the fact states uses obsolete tactics, which often defy on the democratic institutions, but what is more than important to discuss is to what extent, digital technologies open the doors for new opportunities for public bodies. This chapter is based on the study case of No 10 Downing Street e-petitions Initiative that engage lay-citizens to take an active role in the process of security within established democratic institutions.

Chapter 7 triggers a hot-debate in the last chapter of the second section, examining the Matrix Saga as the precondition to understand how the meaning of reality can be politically tergiversated to discipline the citizenry. Matrix represents more than a film, it exhibits an old concern from philosophers to harmonize the counter-and-balance powers of democracy with the need of security.

Chapter 8 echoes the original concerns of NSC (National Security Council) in view of the rise of computers, software and technologies which can be disposed towards criminal acts. Per these specialists, cyber terrorism has the same or worse disastrous effects than classic terrorism. This chapter provides a conceptual discussion on three different arguments respecting to cyber-terrorism, which merits to be included in this project.

Chapter 9 discusses the problems of democracy to articulate individual civil rights to protest, with civil chaos. This work focuses on the rise of civil disobedience as a political factor to produce political instability, which in some condition can be functional to some terrorist cells. Dialoguing with Rawls and other philosophers about the nature of state, Crosston devotes considerable resources to find a valid solution to the dichotomy between surveillance vs. democracy. The same applies for the use of Twitter that proved to be a valid instrument for channelling social discontent in developed and underdeveloped nations.

Chapter 10 sheds light on the problem of social discontent and digital technologies. The culture of protest found in twitter a good ally, since the mobilization of masses turned easier in our times, in view of the rise of informational technology or ICT than the society of our parents. Though at a preliminary stage, governments should control social media in order to protect their citizens, providing health services or medical care in the protest, it is safe to say that these protests evinces serious political crises in view of the public discredit politicians and leaders suffer.
Chapter 11 centres on what specialists dubbed as “the irony of democracy”. The dilemma says that social order is convened by means of the introduction of lesser-evil doctrine. As it was originally discussed by Michael Ignatieff, terrorism and “the war on terror” undermined the democratic institutions as well as the autonomies of branches and agencies. Sociologically speaking, the roots of our current atmosphere of terror come from our incapacity to understand its connection with rationality. Indeed, beyond the polemics terrorism has woken up in recent decades, a much deeper discussion is necessary to understand that terrorism and economy are inevitably entwined. Here, I toy with the idea that in the society of “terror”, the inflation of risk in charge of mass media not only contributes to the formation of an omnipresent state but also engenders a neo-individualism (universalism) which leads very well to substantial changes in pre-existing jurisprudence. The paradox lies in the fact in the name of human right violations; the doctrine of lesser evil is eroding the basis of Athenian democracy.

Hopefully this guide-book helps readers to understand not only the problem of terrorism, but also the role of technology as a double-edged sword to protect citizens. I would thanks IGI global for the opportunity to publish this project as well as all well-reputed authors and contributors who have done of this a masterful work, highly recommended by scholars, policy makers and students concerned by topics of this calibre.

Maximiliano E. Korstanje

University of Palermo, Argentina & University of Leeds, UK

Buenos Aires, Oct 19 of 2016

REFERENCES


