Terrorist use of the Internet:
an analysis of the current threat and its potential evolution

Matteo Cavallini

Technical Report
RHUL–MA–2014–11
01 September 2014

Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX,
United Kingdom

www.ma.rhul.ac.uk/tech
Terrorist use of the Internet: an analysis of the current threat and its potential evolution.
Table of Contents

Executive Summary
Introduction
Literature Review

1 – Terrorism, a phenomenon with various definition

2 - Terrorists who use Internet and Cyberterrorists: two different criminal categories

2.1 – Terrorists who use Internet: different ways to use Internet to support terrorist activities
2.2 – Cyberterrorism: what to expect in the near future

3 – Internet as a communication mean

3.1 - The publicity: Websites, videos, forums chatrooms and social networks
3.2 – The secrecy: cryptography, steganography and other approaches

3.2.1 - Naive approaches to secrecy
3.2.2 - Real cryptography: Mujaheddin secrets, TOR and TrueCrypt
3.2.2 - Steganography

4 – Internet as a way to fund groups and cells

4.1 - Main funding sources
4.2 - Money laundering and ways to transfer funds

5 – Internet and the new opportunities for terrorists

5.1 - Maps, geolocalization and smartphones
5.2 - Information gathering
5.3 - Simulators and augmented reality

6 - Cyberterrorism

6.1 - Hacktivism or terrorism

6.1.1 - Is DDoS always only a form of protest?
6.1.2 - Other forms of protest or other attacks?
6.2 - Targets and scenarios

6.2.1 – Critical infrastructure and SCADA systems
6.2.2 – Threat and vulnerabilities of the energy sector
6.2.3 – Are the transportation systems really at risk?

6.3 – New opportunities for the cyber-terrorists

6.3.1 - Crimeware: exploit kit, botnet e financial malware
6.3.2 - Cyberweapons: the future of terrorist attacks?
6.3.3 - SWATing and TDoS

6.4 – Assessing the risk of such an event
6.4.1 – Description of the risk assessing method

6.4.2 – The cyber terrorist scenario

6.4.3 – The results of the risk assessment

7 - Conclusion

Bibliography

List of figures & tables

Figure 1 - Image of an article published in the magazine Inspire (Hypponen, M.)
Figure 2 - GUI of “Mujaheddin Secrets” (Danchev, D.)
Figure 3 - The layout of a standard TrueCrypt volume before and after a hidden volume was created within it. (TrueCrypt official website)
Figure 4 - A screenshot taken from the Long War Journal website (Joselyn, T. 2013)
Figure 5 - A photo taken from the article “Google Buys Image and Gesture Recognition Company Viewdle” Ningauble, 2012
Figure 6 - An image taken from the video "AiRScouter" see-through type head-mounted display of Brother, (2011)
Figure 7 - An image taken from the blog post “Under the Hood of the Cyber Attack on U.S. Banks” (Atias, 2013)
Figure 8 - The attack distribution among critical infrastructure sectors (ICS-CERT, 2013)
Figure 9 - A screenshot of the vulnerable web-server in which are accessible the ENEA-ENEL project documents (2013)
Figure 10 - A screenshot of the Home page of the management console published by Schneider Electric (2013)
Figure 11 - An example of the information that can be accessed using the Schneider Electric’s website (2013)
Figure 12 - The article about the possible job reduction in the Schneider Electric’s plant (2012)
Figure 13 - A modification of the “Determination of the likelihood” taken from NSSM document
Figure 14 - A modification of the “Risk Diagram” taken from NSSM document with the insertion of the Cyber terrorist scenario.
Figure 15 - Priority Risks taken from the UK National Security Strategy.
Executive Summary

This project report is aimed at analysing the present and future use of the big Internet by terrorist groups, with a particular interest in the understanding of the possibilities to realise a cyber attack.

Terrorist groups have been able to adapt their strategies to all specific contexts in which they decide to operate; the use of Internet represent one good example of their capacity to model their strategies. Internet is used in almost every way to give a direct or indirect contribute to terrorist operations. In this research I report examples of a lot of these different approaches to use Internet such as the following:

- realisation of campaigns to raise up the consensus around a cause;
- diffusion of text and video messages bypassing the filter of the traditional media;
- solicitation on giving help and money;
- realisation of more efficient ways to transfer and launder the money;
- creation of forums where share ideas, knowledge and initiatives in a secure way;
- diffusion of manuals and materials to give the basic knowledge in the preparation of an attack;
- combination of cryptography and steganography to communicate secretly and securely
- use of navigators, on-line maps, smartphones and new tools to prepare and conduct operations in field.

Then, looking at the next future, I also explored the new possibilities opened by the technology such as the use of malware or cyberweapons to realise attacks that multiply their effects by the use of Internet or the evil use of a tool such as the Google Glass to support the operations of an active terrorist cell.

Finally in this research I explored the possibilities to realise a cyber terrorist attack, evaluating the pros and cons in such kind of scenario. In this topic I found some blurred elements that, at the light of some definitions of cyberterrorism, could be considered some first elementary examples of such form of attack.

At the end I assessed the risk of a big cyber attack using a methodology derived by the UK National Security Risk Assessment (NSRA) and the National Security and Safety Method (NSSM) of the Netherlands, finding that this kind of risk has a value comparable to some more “traditional” big
terroristic attacks and hence this kind of events should be investigated better by the national and international bodies to fully comprehend their real significance.

**Introduction**

This project report is aimed at analysing the present and future use of the big Internet by terrorist groups, with a particular focus on the characteristics and issues of cyberterrorism in the future.

In order to maintain a concrete and easily verifiable project profile I have used real cases as much as possible to start the analysis and evaluation. In particular the objective of this project is to answer to the following questions:

- What is the current use of the Internet by terrorists?
- What are the possible evolutions of this use?
- Is it always possible to distinguish between hacktivism and terrorism?
- What are the possible targets and scenarios for cyberterrorism?
- Is cyberterrorism a credible threat for the near future?

In the first two chapters, I will give a general description of the terrorist phenomenon starting by defining and clearly distinguishing between: the use of Internet as a supporting tool for terrorist activities, and the use of internet as weapon in itself to perform real attacks.

The third chapter will be devoted to the possibilities that terrorist groups have to use Internet as a way to directly communicate their messages towards the public and, on the other hand, to use Internet as a very secret way to communicate among cells.

The fourth chapter will briefly treat the ways to collect money to fund the terrorist activities and the methods to transfer the money to the final users.

In the fifth chapter I will analyse the possibilities opened by new technologies and new ways to use Internet by terrorists with a particular attention to the evil side of some innocuous tools.

The sixth chapter will be the most complex and articulated of the entire project and will be devoted to cyberterrorism. This theme will be analysed to highlight the concrete possibilities of the realisation of such actions and to spot the soft targets that could be attacked. The chapter ends with an analysis of the likelihood of such events.

In the final chapter I will draw the conclusion of the project highlighting the importance of truly understanding the present use of Internet by terrorist groups in order to hypothesise future threats and new scenarios.
Literature Review

My project was developed using texts and papers published by national and international bodies, research performed by academics, and materials produced by independent security research.

The main sources for my research project are:

- United Nations Office on Drugs and Crime (UNODC)
- Counter-Terrorism Implementation Task Force (CTITF)
- Europol
- NATO - Centre Of Excellence - Defence Against Terrorism (COE-DAT)
- National security bodies (UK, Italy, Netherlands)
- Istituto di Altı Studı della Dıfesa (IASD), the institute of high defence studies from Defense Joint Staff
- Presidenza del Consiglio dei Ministri - Sistema di Informazione per la sicurezza della Repubblica, the Italian intelligence agency
- Academic publications
- Council of Europe
- Journalists and independent security researchers

1 – Terrorism, a phenomenon with various definition

Modern terrorism is a relatively recent but very complex phenomenon. As reported by Wikipedia (2012), one of the ideologies behind using terrorism to achieve political objectives, originates in Europe in the beginning of the 19th century with:

"the "Propaganda of the deed” (or "propaganda by the deed," from the French propagande par le fait) theory, a concept that advocates physical violence or other provocative public acts against political enemies in order to inspire mass rebellion or revolution. One of the first individuals associated with this concept was the Italian revolutionary Carlo Pisacane (1818–1857), who wrote in his "Political Testament" (1857) that "ideas spring from deeds and not the other way around.” Anarchist Mikhail Bakunin (1814–1876), in his "Letters to a Frenchman on the Present Crisis" (1870) stated that "we must spread our principles, not with words but with deeds, for this is the most popular, the most potent, and the most irresistible form of propaganda."

Current terrorism well reflects this kind of approach and Internet is the perfect way to vehiculate the news about the “deeds” and also the terrorist ideology.

In its evolutions, terrorism presents a varied phenomenology so the very long list of its definitions
takes in account this complexity. Moreover, throughout time many governments were tempted to stick the label of terrorism on their enemies and in doing so they stretched and modified its definition in order to achieve their desired result. Finally, the terrorist groups themselves modified their behavior, tactics and methodology many times over the course of time thus forcing institutions to change their definitions of this elusive phenomenon.

The result of such an evolution is the production of over one hundred different definitions of terrorism.

However, despite the total number of definitions, some of them are now well recognized and accepted. For example the definition of “terroristic act” in Art.1 of the “EU Council Framework Decision of 13 June 2002 on combating terrorism” is used as a basis in all the legislation of the Member States of the European Union. In this article terrorist offences are defined as:

“acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:

— seriously intimidating a population, or

— unduly compelling a Government or international organisation to perform or abstain from performing any act, or

— seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation,

shall be deemed to be terrorist offences:

a. attacks upon a person's life which may cause death;
b. attacks upon the physical integrity of a person;
c. kidnapping or hostage taking;
d. causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
e. seizure of aircraft, ships or other means of public or goods transport;
f. manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
g. release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;
h. interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;
Another important definition is given in the Art.2 of the UN “International Convention for the Suppression of the Financing of Terrorism” which defines an act of terrorism as:

“act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act”

It is quite easy to spot the obvious differences in these two definitions. The consequence of such variability in the definitions makes it very difficult to situate a new and “innovative” approach to terrorism such as cyberterrorism.

Gathering the common parts of these definitions is the way in which some researchers have tried to compose a more accepted description of the phenomenon. An example of this kind of effort is the definition produced by Boksette C. (2008) in which:

“Terrorism is defined as political violence in an asymmetrical conflict that is designed to induce terror and psychic fear (sometimes indiscriminate) through the violent victimization and destruction of noncombatant targets (sometimes iconic symbols). Such acts are meant to send a message from an illicit clandestine organization. The purpose of terrorism is to exploit the media in order to achieve maximum attainable publicity as an amplifying force multiplier in order to influence the targeted audience(s) in order to reach short- and midterm political goals and/or desired long-term end states.”

2 - Terrorists who use Internet and Cyberterrorists: two different criminal categories

After examining the growing interest of subversive movements to use the net to carry out their tasks, many analysts recently hypothesized that the conditions to exploit the Internet as a weapon are approaching. It has to be highlighted, however, that a big difference exists between the use of Internet to support the terrorist activities and the use of Internet to perform attacks. Only the latter can be fully defined as a cyberterrorist act.

In fact, as it is extensively explained, the prerequisite to call an event “cyberterrorism” is the use of Internet to produce violence and/or physical effects, comparable to those created by a kinetic attack. Having this perspective clear in mind it is apparent that terrorists and cyberterrorists are different categories of criminals who have different skill sets and different views regarding targets. It is also apparent that, at the moment, the conditions to perform a cyberterrorist attack are yet far from reality.
2.1 – Terrorists who use Internet: different ways to use Internet to support terrorist activities

Internet is a tool that, in little more than twenty years, has resulted in a big change in the real life of everyone modifying the lifestyle of people, companies and government. Terrorist groups were not immune to these changes. Initially, they developed some capabilities at the individual level only to evolve later toward a more structured approach in their use of Internet. Some authors (Olimpio, 2008) even state that the expansion of Al-Qaida would not be possible without the use of Internet.

At the same time, however, also the intelligence and law enforcement agencies in every country developed Internet based tools to monitor terrorist activities and to perform more complex and effective investigations.

At the moment, the main uses of Internet for terrorist purposes are related to the following:

- diffusion of terrorist propaganda;
- radicalisation and proselytism;
- collection and transferring of funds;
- diffusion of materials related to preparation of attacks;
- coordination of activities and the exchange of secret messages;
- information and intelligence gathering;
- support during the preparation and the executions of attacks.

All these activities however leave traces that are followed by the law enforcement agencies in a never ending battle to foil the planned atrocities before they happen.

As a matter of fact, this reality forced the terrorist groups to attempt to use Internet in such a way that would offer the minimum attack surface for the infiltration and investigation of law enforcement and at the same time continue to use Internet to communicate within and outside the cells. Hence, for terrorists the real dilemma to solve became finding a way to attract publicity and to maintain secrecy at the same time.

One of the solutions recently adopted by Al-Qaida, is the incitation to the so called “individual jihad”, in which the interaction between the operative cells (or the lone terrorists) is minimal because the radicalisation materials and the necessary instructions to set up a basic form of attack are widely diffused on Internet. Sadly, as we have seen ourselves in the last few months for example with the case of the Boston Marathon attacks, this kind of approach has proven to have a great capacity in the realisation of simple attacks with a high potential to affect the feeling of the population and diffuse fear.

Finally, the effectiveness of the use of Internet for radicalisation was understood by all the subversive organisations, in fact, as noted by the United Nation Counter-Terrorism Implementation Task-Force (CTITF) in 2009:
While Al-Qaida is highly sophisticated in its use of the Internet, it is not unique. Websites and forums are used by almost all terrorist organizations, and sophisticated video productions can be found on the Internet from a number of politically violent groups (Videos, music and similar materials expressing support for politically violent groups as diverse as, for example, ETA, the PKK, the Tamil Tigers, FARC-EP and The Naxalites, can be readily found on the Internet.).

2.2 – Cyberterrorism: what to expect in the near future

As it is supported by a lot of real cases, it is easy to verify that the use of Internet by terrorists groups is very practical. They try to exploit the potential of this technology while minimising the related vulnerabilities. So though they are aware that the cyberterrorism could be fundamental in the future they also know that, at the moment, an attack based on the use of the net is out of their reach. In fact, EUROPOL, in the report “Counter Terrorism Working Group Conclusion” (2011) states that:

“The internet will not only be used as a tool for recruitment, training, planning, as well as being a potential target itself but will also be used as a weapon, for instance on critical infrastructure, and for intelligence gathering. Terrorists will always study and invest in new technologies in any way possible to facilitate their activities, but the traditional means of attack will remain an easy, cost-effective option for the near future.”

In the late 90s/early 2000s, due to the increasing dependency of the world on the Internet resources, researchers have started to analyse seriously the use of Internet as a way to perform attacks, so the terms cyberwarfare and cyberterrorism have become very common and frequent. But, as we saw in the previous paragraphs, there are many different views about what terrorism is and in the same way there are a lot of different views about what cyberterrorism is. This blurriness originates a multitude of definitions with a lot of differences from one to another. For example, as reported by Kerr K. of the AusCERT (the Australian Computer Emergency Response Team), the US National Infrastructure Protection Center defined cyberterrorism as:

“a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda”

Pollit M., FBI special agent, proposed a definition that extends the concept expressed in the previous definition. Pollit indeed wrote:

“Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents.”

Finally, as reported by the “Centre of Excellence – Defence against Terrorism”, NATO proposed the following definition in which there is an explicit waiver to the use of the term “violence” in
favor of the more blurry concepts of “destruction” and “disruption”. NATO definition in fact is:

“A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.”

As previously noted, at the moment, there aren’t the right conditions to perform a terrorist cyberattack in the real world, but taking into consideration the evolutionary rate of the use of Internet for terrorist purposes the researchers and community of experts think that it is just a matter of time and no longer a mere academic hypothesis.

3 – Internet as a communication mean

As stated in Boksette’s definition of terrorism, the publicity of an attack is almost as important as the attack itself. Indeed, some attacks have been perpetrated just because there was a message to communicate via the media exploitation. From this perspective, Internet has been a game changer because it enables terrorist groups to:

- communicate directly to the intended audience bypassing the filter of the journalists;
- expand enormously the exposition of the messages;
- reach almost every single would-be terrorist or supporter.

This capability has reached its apex with the rise of Web 2.0, an approach to content publication in which the boundary between the audience and the information producer is blurred and interchangeable. Multimedia tools such as photo, video and audio led to the realisation of “professional” communication campaigns and by taking advantage of blogs, social networks, websites, forums and chatrooms, terrorists can have at their disposal all the needed tools to recruit and manage the new generations of operatives. So, terrorist groups have started to specialize part or their resources on the use of Internet to expand their capabilities and multiply the effects of their actions. As noted by Denning (2010) in “Terror’s Web: How the Internet Is Transforming Terrorism”:

“Superficially, terrorists use the Internet in pretty much the same way that other individuals and groups use the Internet. They use it to communicate amongst themselves and to reach out to supporters, the media, governments, and the public. They use it to exchange messages and engage in online discussions. They use the net to distribute information, including text, images, audio, video, and software, and to find information. They use it to learn, transact business, and generally facilitate their activities. And, like other bad actors on the Internet, they use the net to inflict harm. Yet from this seemingly normal usage, the very practice of terrorism is being transformed. This transformation takes the form more of an expansion of options and activities rather than a replacement of traditional ways of operating.”
3.1 - The publicity: Websites, videos, forums chatrooms and social networks

The majority of terrorist formations have well understood the importance of the use of Internet to create attention and to spread their message, and have created a huge number of websites and forums to support their activities. As reported by Ramsay G. (Defence Against Terrorism Review, 2009) around 2008, the total number of the terrorist related websites is ranging between 5,300 (Gabriel Weimann ‘The Psychology of Mass-Mediated Terrorism’ American Behavioural Scientist Vol 52, No 1, 2008 pp. 69-86) and 50,000 (Eric Swedlund, ‘UA effort sifting web for terror threat data’ Arizona Daily Star 24/09/2007). The FBI in a 2009 report estimates that at that time there were roughly 15,000 terrorist websites of which 80% were hosted in the U.S. (Ryan, J. 2010). These numbers have been increasing over the years and current evaluation are now in the upper range of the previous numbers.

Many real cases have shown that the use of Internet has been fundamental in the radicalisation process and in the subsequent recruitment of extremists and terrorist. For sure, one of the most emblematic is the Roshonara Choudry case (Dodd, V.) who in 2010 was sentenced for the attempted murder of a Member of Parliament, Stephen Timms. In one of her declarations, Choudry, previously a brilliant english student well integrated in the society, affirmed that she decided to kill a Member of Parliament as an extreme act of protest against the UK’s participation in the Iraq war. Investigators analysing her computer showed that the process of her transformation had started only six months prior to the day of the attack.

By her admission (Cavallini, 2013), her radicalisation process was due to:

- sight of Anwar al-Awlaki’s videos (al-Awlaki, also known as “Bin Laden of the Internet”, published a huge number of islamist videos and text. He was killed with other Al-Qaida terrorists in Yemen during a US drone attack)
- sight of Abdullah Azzam’s videos (Azzam, also known as “Father of the Global Jihad”, was the inspirer and mentor of Osama Bin Laden)
- consultation of the jihadist website www.revolutionmuslim.com (at that time this website, was hosted in US servers and it was used to publish links, speeches, texts and videos to promote the jihad)

This episode is emblematic but, sadly, not unique and this kind of use of Internet resources doesn’t belong only to the islamist groups but, as noted before, almost all terrorist and extremist groups have an Internet presence. For example, also right wing extremists use mainly the publication of White Power Music videos to spread their xenophobe messages (Europol TE-SAT, 2012) and as noted by the Italian Department of Information and Security in the “Relazione sulla politica
dell’Informazione per la sicurezza” (Report on the policy of information for security) (2013): “In the last few years we have seen a growing interaction between the most radical groups (Germans, Austrians, Spanish, Swiss and Scandinavians). The use of Internet plays a relevant role in the diffusion of xenophobe messages and in the recruitment of new supporters. The interactions among different right wing extremist groups are facilitated by the lack of an homogeneous legislation in all European countries.

As reported in the UNODC paper (2012), two other real cases are worth a mention: the Y. Tsouli case and the Hicheur case. The first one regards an individual, also known as Irhabi007 (Terrorist 007), who was sentenced to 16 years in prison to have created a lot of websites diffusing information about:

- preparation of terrorist attacks, including the preparation of suicide bomb vest,
- radicalisation material along with videos of terrorist attacks, including decapitations of kidnapped hostages.

The second case, regards a French nuclear physicist who was sentenced to 5 years of prison for having acted as a moderator in a jihadist website and for taking concrete steps to provide financial support to Al-Qaida in Islamic Maghreb”(AQIM).

Finally it is important to note that forums and chatrooms have been more important for terrorists groups than websites. In fact, the possibility to interact and establish a real communication between supporters is a crucial factor for the success of the terrorist use of Internet.

3.2 – The secrecy: cryptography, steganography and other approaches

From a security perspective, the terrorist use of Internet tools to assure the secrecy of their communications is one of the most controversial and fascinating aspect of the entire relationship between terrorists and Internet. There are real cases which show that some islamist groups, in less than ten years, despite their initial refusal to use internet technology at all they have managed to arrive at a very sophisticated use of cryptography and steganography. In fact, as mentioned by Denning (2010):

“the „Al Qaeda Training Manual,“ found by British police and released by the Department of Justice in 2001, says nothing about computers, software, the Internet, cell phones, satellite phones, or other modern information technologies known to be used by al-Qaida. The section on secret writing and ciphers (lesson 13) makes no mention of modern cryptographic systems and is based entirely on manual methods that appear to be at least 50 to 100 years old.”

On the contrary, the present situation is characterized by a large use of sophisticated tools to ensure
anonymity and confidentiality such as TOR (The Onion Router) or “Mujaheddin secrets” (see paragraph 3.2.2). However, many researchers (David B. reporting Campbell D. speaking at DeepSec conference, 2012) point out that these sophisticated cases are not representative of the real average terrorist user.

3.2.1 - Naive approaches to secrecy

Frequently, there is an association between islamilist ideology and the repudiation of modern technology. Indeed, technology is associated with the western (and in their view, corrupted) lifestyle and therefor would entail a complete and aprioristic refusal on the part of the islamilist terrosrist. In fact, this situation has curbed the diffusion of modern cryptography and a mature IT approach to secrecy. However, in the real world, it is near impossible to maintain a relationship with someone whether they be two cities away or two plane rides away without using modern communication tools such as emails and attachments. This conflicting situation can sometimes lead to the adoption of naive solutions that highlights their lack of comprehending the set of problems inherent with trying to keep secrets on the internet and their lack of ability and confidence when it comes to the art of cryptology.

The Rajib Karim case is a good example of this naive approach to secrecy. Karim (Dodd, V., 2011) was a British Airways employee who was convicted for fundraising for a terrorist organisation. Moreover, he had been in touch with Anwar al-Awlaki (as recalled in the previous paragraphs he was a well known leading figure of the Al-Qaida), with whom he exchanged a lot of compromising messages. Aware of the necessity to find a solution to guarantee the confidentiality of their communication, and despite Awlaki’s suggestion to use the encryption tool “Mujaheddin secrets” (see next paragraph), Karim adopted his own custom solution. (Mcdonald, A. and Bryan-low, C.) This was his composite approach:

- he used a website to exchange files instead of a public email system;
- he encrypted the files to exchange with the software Pretty Good Privacy (PGP);
- he created a shift cipher to encrypt the texts, using Microsoft Excel;
- he used an exchanging method to avoid the use of real names and places, or compromising words.

All his efforts were worth nothing. After nine months of work the messages were brought back to the investigators completely decoded by the British intelligence services. Although his approach to cryptography was defined as sophisticated by some journalist and investigators, it denotes a lack of general comprehension of the mechanics of crypto combined with a mistrust of the open source tools that are normally used to encrypt files and messages. In particular, he missed the importance
of using:
- verified encryption programs without known vulnerabilities
- very strong passphrase

In fact the robustness of his solution relied solely on the encryption realised by PGP because the shift cipher doesn’t add any real contribution to the security of the messages as it is easily breakable using a statistical approach. Moreover, using a substitution mechanism to avoid the use of compromising terms is only of value in so much as it manages to avoid detection and alludes the attention of law enforcement, but it holds almost no value whatsoever when it is used within an encrypted message.

Finally, the avoidance of the use of public email systems is a common trait of many terrorist plots and it has to be seen as a mere way to try to circumvent some automatic alert systems but has a very limited value in the case of an investigation.

3.2.2 - Real cryptography: Mujaheddin secrets, TOR and TrueCrypt

Besides the naive approaches recalled in the previous paragraph, there are other cases in which terrorists use effective cryptographic tools to communicate secretly and to store confidential information. In this field, it is worth noting the efforts invested in the development of one comprehensive crypto tool (also in arabic language) which encompasses within it a whole collection of open source cryptographic tools. This activity is aimed at introducing a terrorist tool that is directly linked to and approved by Al-Qaida in the hope of overcoming the previously mentioned wariness in the use of cryptography by the islamist extremists. This tool is named “Mujaheddin Secrets” and it is currently available in version 2.0.

Some authors still doubt the authenticity of this tool, viewing it as a “trojan” created by western intelligence services. However we do find some endorsement by al-Awlaki (as in the reported Karim case) and by some articles in the magazine “Inspire” (see image below) that give a clear idea about the authorship of this tool.
As reported by Dancho Danchev, Mujaheddin Secrets version 2.0 (also “Asrar el Mojahedeen” in the arabic version) was released by the Global Islamic Media Front (GIMF) in 2008 and this tool represents a serious improvement of version 1.0 in terms of functionality and in terms of ease of use. In fact, the following are the features of both versions:

**Key features in the first version:**
- Encryption algorithms using the best five in cryptography. (AES finalist algorithms)
- Symmetrical encryption keys along the 256-bit (Ultra Strong Symmetric Encryption)
- Encryption keys for symmetric length of 2048-bit RSA (husband of a public key and private)
- Pressure data ROM (the highest levels of pressure)
- Keys and encryption algorithms changing technology ghost (Stealthy Cipher)
- Automatic identification algorithm encryption during decoding (Cipher Auto-detection)
- Program consisting of one file Facility file does not need assistance to install and can run from the memory portable
- Scanning technology security for the files to be cleared with the impossibility of retrieving files (Files Shredder)

**New features introduced in the second version:**
- Multicast encrypted via text messages supporting the immediate use forums (Secure Messaging)
- Transfer files of all kinds to be shared across texts forums (Files to Text Encoding)
● Production of digital signature files and make sure it is correct
● Digital signature of messages and files and to ensure the authenticity of messages and files”

As it possible to see in the following image, the Graphical User Interface (GUI) is very simple and it enables the use of cryptographic functions without any particular skills.

![GUI of “Mujaheddin Secrets”](image)

**Figure 2 - GUI of “Mujaheddin Secrets” (Danchev, D.)**

The real use of this tool was proven in court in the Hicheur case (UNODC). A French court proved that Hicheur used the Asrar encryption function to produce encrypted files to distribute them via Rapidshare in support of his terrorist activity.

The anonymizer tools are another class of tools well known by terrorists. UNODC, in the recalled 2012 report, stresses on the importance of the use of “The Onion Router” for masking the source IP address used to communicate by terrorists. TOR bounces the communications around a distributed network of relays run by volunteers all around the world giving the chance to an Internet user:

● to prevent somebody from finding out what sites are visited;
● to prevent the visited sites from finding out the physical location of the user.

In fact, UNODC wrote about the use of TOR:

“For example, applications such as The Onion Router may be used to protect the anonymity of users by automatically rerouting Internet activity via a network of proxy servers in order to mask its original source. Rerouting network traffic via multiple proxy servers, potentially located in different jurisdictions, increases the degree of difficulty of accurately identifying the originator of a transmission.”
As further consideration about the use of TOR, I think that it is important to also mention another open source project, a Linux distribution named “Tails - The Amnesic Incognito Live System”. This is a USB (or DVD) Linux live distribution, based on the well known Debian distro with the addition of an embedded use of TOR for external communications and the complete renunciation of the use of the PC’s hard-disk. In Tails official website there is a clear statement about the main functionality offered by this live distro:

“Using Tails on a computer doesn't alter or depend on the operating system installed on it. So you can use it in the same way on yours, the computer of a friend or one at your local library. After removing your Tails DVD or USB stick the computer can start again on its usual operating system.

Tails is configured with a special care to not use the computer's hard-disks, even if there is some swap space on it. The only storage space used by Tails is the RAM memory, which is automatically erased when the computer shuts down. So you won't leave any trace neither of the Tails system nor of what you did on the computer. That's why we call it "amnesic".

This allows you to work on sensitive documents on any computer and protect you from data recovery after shutdown. Of course, you can still explicitly save some documents to another USB or external hard-disk and take them away for future use.”

It is worth noting that Tails has the possibility to be launched with a graphic interface that very much resembles the Windows XP GUI, thus enabling the user to launch it in public places without giving rise to any suspicion. That makes this tool the ideal companion for the terrorist who likes to use Internet cafè to communicate in a very confidential way. Moreover, the use of Tails and TOR give access to a hidden part of Internet, the so called “Dark Web” in which a lot illegal activities are running and it is possible to find any kind of resources in a complete anonymity.

In my opinion, the last tool that has to be mentioned is TrueCrypt, another robust and well documented open source project aimed at distributing a free encryption tool. Beside the robustness of the solution, there is a specific feature that distinguishes this tool from the other cryptographic tools: the possibility to create a so called “Hidden Volume”. The following is what it is written in the official TrueCrypt website regarding this feature:

“It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
The principle is that a TrueCrypt volume is created within another TrueCrypt volume (within the free space on the volume). Even when the outer volume is mounted, it should be impossible to prove whether there is a hidden volume within it or not*, because free space on any TrueCrypt volume is always filled with random data when the volume is created** and no part of the (dismounted) hidden volume can be distinguished from random data. Note that TrueCrypt does not modify the file system (information about free space, etc.) within the outer volume in any way.”

It is apparent how such a feature can be useful for a suspect of terrorism to conceal compromising information regarding his/her illicit activity and this capability certainly did not slip past the UNODC which briefly mentioned it in its report.

3.2.2 - Steganography

Steganography is the science of secret writing and has a long history that started in the Middle Ages. As reported by Wikipedia, modern steganography

“includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.”
Changing the least significant bit of a range of pixels, steganographic tools leverage the limited capacity of the human eye to perceive the slight differences in images, this makes steganography a powerful tool for exchanging secret information without giving rise to any suspicion. Indeed, the direct use of cryptography is per se something that makes a file suspicious for an investigator’s eye. Using a layer which disguises the cryptography allows for the exchange of these kinds of suspicious files to go unnoticed.

There are a lot of cases in which steganography was used to conceal messages and communication between terrorist groups, the most relevant in my opinion are the following two cases (Cavallini, 2013).

The first example was Italy in 2004, where after a very complex police operation (as reported by newspapers (Corriere della Sera, 2004), the “Operation Tracia” which was 18 months long and entailed: phone wiretapping, physical and digital interceptions, shadowings and an important work of digital decoding) 82 alleged terrorists were arrested in Turkey and an additional 54 in Belgium, Greece, Germany and in the Netherlands and 5 more in Italy. They were all part of the Turkish left wing terrorist formation DHKP-C. In this case UNODC reports that the terrorist used the steganographic tool “Camouflage” to hide encrypted data within images (JPEG and GIF) exchanged via email systems. In this case, the Italian Carabinieri of the Raggruppamento Operativo Speciale (ROS) who carried out the investigation were able to gather or intercept encryption passwords and with a further complex forensic analysis to then identify and recover the hidden messages.

Another example of the use of steganography for terrorist purposes is seen with the arrest of a suspected member of Al-Qaida in Berlin. Maqsood Lodin, a 22 year old, Austrian, on the 16th of May 2011, was stopped and questioned by the German Police, after traveling to Berlin from Pakistan via Hungary (Infosecurity, 2012). He was found to have a memory stick hidden in his underpants and as reported in 2012 by Gallagher S.: "he was found with a memory card with a password-protected folder—and the files within it were hidden. But, as the German newspaper Die Zeit reports, computer forensics experts from the German Federal Criminal Police (BKA) claim to have eventually uncovered its contents—what appeared to be a pornographic video called "KickAss." Within that video, they discovered 141 separate text files, containing what officials claim are documents detailing al-Qaeda operations and plans for future operations—among them, three entitled "Future Works," "Lessons Learned," and "Report on Operations." So just how does one store a terrorist’s home study library in a pirated porn video file? In this case the files had been hidden (unencrypted) within the video file through a well-known approach for concealing messages in plain sight: steganography.”

Storing information in a video means a lot of free space to hide messages and the added possibility
to use different channels such as, audio, video and transitions to create even more space. To detect and recover information that is otherwise concealed by steganographic tools is not too difficult as long as the investigators have some suspicion that such tools have been used. However, if a combination of cryptography and steganography is used, a different investigative approach is needed as the DHKP-C case showed well.

Finally, it is worth reporting that recently a Polish researcher, Mazurczyk W. at the Institute of Telecommunications in Warsaw, presented a project named SkypeHide by which it is possible to use the silence moments in a Skype calls to exchange secret data (Marks, P. 2013). In fact Skype, rather than send no data between spoken words, it sends 70-bit-long data packets instead of the 130-bit ones that carry speech. The receiver ignores the packets carrying secret messages that are decode by the SkypeHide component. Since these secret packets are indistinguishable from silence-period traffic, their detection is very hard. The project will be presented at a steganography conference in June 2013.

Each one of the above mentioned tools is a very powerful element that could be used by terrorist groups to hide secret messages. Knowing the range of tools the terrorists have to work with, it would be very desirable at this point to set an international standard procedure aimed at discovering these instances and carrying out successful investigations.

4 – Internet as a way to fund groups and cells

The relationship between Internet and funding terrorist formations is complex but, in essence, there are three main activities in which Internet plays a fundamental role:

- fundraising
- money laundering
- money transferring

Fundraising of terrorist formations via Internet is now an ascertained fact. Terrorists use Internet to spread their message and sollicite radicalised people and magnates to donate some money for their cause. Therefore many terrorist websites are devoted to this objective and some countries are very concerned for the presence these websites because it is very difficult to control them. In fact, many contrasting measures such as the closing of the websites are often ineffective or worse could be qualified as censorship.

Beside solicitation to donate some money for their cause, many terrorist formations use more
“creative” ways to realise their fundraising through Internet for example practising carding\(^1\) or selling computer games with extremist contents (UN-CTITF, 2009).

In the next paragraphs I will analyse the current scenario in which these illegal activities are carried out and I will describe some possible evolutions to expect in the near future.

4.1 - Main funding sources

Terrorist fundraising campaigns on Internet can be divided in three main typologies: direct solicitations, e-commerce and the illicit use of online payment systems.

Regarding the direct solicitations, terrorist formations can use Internet as a mean to create real “marketing campaigns”. Online tools are so sophisticated and easy to use that the realisation of an effective website to collect funds is something within everybody’s reach. Many studies showed (Burke, 2009) the efficacy of solicitation campaigns mostly when videos are used and for example this is one of the reasons why terrorists and insurgents invested so much energy in recording attacks during the Iraq war. In this case, the combination composed by video-cameras, PCs and Internet tools was a real game changer which allowed terrorist groups to collect a huge amount of donations and recruit a lot of volunteers. Also social networks were used to maintain these kind of point of presence in the net creating a multi faceted approach to donations.

---

\(^1\) Carding crimes are offenses in which the Internet is used to traffic in and exploit the stolen credit card, bank account, and other personal identification information
E-commerce on the contrary has a more limited importance and it is reported only by few nations (UNODC). The most frequent situation is linked to the sale of goods (CDs, DVDs, computer games, books, etc.) by some terrorist supporting organizations, so that a fraction of the collected money can effectively be sent to the operative groups.

Finally, the illicit use of the online payment methods is one of the most interesting and worrying ways to fundraise terrorist formations because, in my view, it has the wider expansion margins. To analyse this phenomenon we can start from the most clear case proved in a court: the Tariq Al-Daour case. This individual was an accomplice of Y. Tsouli and his main activity was to collect money using stolen credit cards. In the black market he bought roughly 37,000 stolen credit cards along with the personal information needed to use them. Using these cards, Al-Daour was able to finance Tsouli’s online terrorist activity.

In my opinion this case has to be perceived as a wake-up call because the situation can only worsen in the future. In fact, the needed skills to become a cybercriminal are even more modest because it is easy to find black-market actors who sell at very cheap prices the “exploiting kit” and the necessary financial malware to start illegal online operations. Furthermore, there are black-market operators who mimic the legitimate cloud computing providers by selling their tools in a “as-a-Service” form. Indeed, the so called “Malware-as-a-Service” (MaaS) scheme is now fully realised because everybody can easily find a “service provider” for all the pieces of software and the expertise needed to realise a botnet based on a financial malware. For example it is easy to find: the financial malware (Zeus, SpyEye, Citadel, etc.), the exploit kit (BlackHole, Phenix, Elenoir, etc.) and the infection service, all sold in forms of services usable also by attackers who are not IT or security experts. Then a would-be terrorist or supporter can propose himself to his referents to become an operative able to gather a lot of money in a short time and this would be very appreciated by many terrorist formations. Supporting this vision there is the statement (Holehouse, M. 2012) of Commissioner Adrian Leppard, head of City of London Police who said:

“There is “plenty of evidence” that al-Qaeda and other terrorist groups are using the proceeds of online fraud to finance their activities. The police and security services are seeking to disrupt those lines of funding.”

Though I were not able to find many evidences for this statement, I know that, in the moment in which there will be a collaboration on a large scale between cybercriminals and terrorist groups, it will be a big problem because identity theft, credit card theft, wire fraud, stock fraud and auction fraud are felonies easy to commit with large profits and lot less risks than other criminal activities. Furthermore, this collaboration will entail also the following “side benefits” for terrorist groups:

- access to the malware used for the identity and data theft;
- introduction with the criminals who develop crimeware (see also 6.3.1);
● opening of new scenarios in which the so called “cyberweapons” are used (see also 6.3.2).

4.2 - Money laundering and ways to transfer funds

Internet is also used as a way to facilitate the distribution of the illegal funds gathered by the supporters of the extremist and terrorist formations. At the moment, one of the main means by which the funds are distributed by terrorists is the so called “Informal Value Transfer System” that is represented by any system, mechanism or set of people who receive money just to pay an equivalent value to someone else in a different geographical location. To avoid to leave traces, the people involved in this form of financial transaction doesn’t have recourse to the conventional banks so, Internet can give a great help to establish and maintain all the needed connections.

Furthermore the following Internet tools are very useful to launder the dirty money:

● electronic currency such as e-gold or Bitcoin; or
● services like Liberty Reserve to transfer the money.

In essence, all the three fundamental operations to launder the money are easier and more effective by the use of Internet. In fact, the “Placement” (the transformation of the real money in virtual money), the “Layering” (the subdivision of the money in many small financial transactions) and the “Integration” (the final recomposition of the sum) with the use of Internet are simplified and made untraceable.

5 – Internet and the new opportunities for terrorists

Internet represented a big change in everybody’s life. Using Internet tools we can obtain a lot of information about people and companies simply using a search engine or connecting to a social network. We can also interact with people and things at a new level via the use of mobile devices and we can easily reach unknown places guided by our smartphones.

This is a world of new opportunities for everyone, unfortunately also for wrongdoers who can leverage these opportunities to create new threats and new attack methodologies. Online tools can enable people to achieve new results and simplify everyday life but this come at the price of the creation of an increasing set of new vulnerabilities and dependencies with the online instruments that are waiting to be exploited by some criminals.

Apparently, terrorist groups aren’t so quick in modifying their consolidated ways to proceed but there are examples that show a multiform reality in which some groups are keen to bring in some important innovations. The Mumbai attack in 2008 is one these. In the next paragraphs I will
analyse some aspects of that attack to show the real possibilities that Internet, cloud and mobile are opening for terrorists.

5.1 - Maps, geolocation and smartphones

One of the most important innovations in our daily life is represented by online maps and GPS navigators and above all those integrated in mobile phones. By the use of these devices we learnt to move through previously unknown places without the necessity to wasting time in precautionary researches or careful plannings. Paper maps are almost completely vanished from our cars and our houses.

This so important innovation has the side effect that a terrorist cell can move and operate in unknown territory with a surgical precision. This fact has been already found on the field during the Mumbai attack. In that bloody attack, a commando composed by ten terrorists was able to move and operate in a city where none of them had ever performed a real field reconnaiss. They were able to execute a very complex operation comprising three main targets (Taj Mahal Hotel, Oberoi Hotel e Nariman House) along with many secondary targets, doing battles with the Indian police firstly and then with the Indian army rushed to stop them. At the end of this folly more the 170 were fallen among civilians and law enforcement agents (Wikipedia, 2013).

During the subsequent trial it was cleared that all of this was possible also because:

- there was a previous accurate planning with the use of Google Earth
- they were able to follow the plan and the established paths with the use of GPS devices
- they were able to react to the police actions using smartphone to know exactly the situation in real time.

Before this attack, the clear vision of the possible evil side of Google Earth or of the use of smartphones was not widespread to general public but was limited to some researchers and military entities. Since this discovery was a shock for the society there were some petitions to ban or limit the information published by Google Earth and Bruce Schneier in an article on the Guardian (2009) explained the dangers of the reactions to these kind of fears. I agree with Schneier’s vision but I think that it is also important to analyse in advance the possible impact of new technologies to have plans in case of an emergencies.

Knowledge and preparedness are the keys to save lives and minimise the impact of an attack.
5.2 - Information gathering

As for anyone, one of the most interesting things that a terrorist can do on Internet is to surf the web looking for some information. Then gaining information about someone or about some target using Internet (such activity is often qualified as OSINT - Open Source Intelligence - or CYBERINT - Cyber Intelligence) is became one of the fundamental steps during the preparation and the planning of an attack. On Internet it is possible to find detailed information about the logistics, the organisation and side conditions of every public place and of the majority of companies and agencies. Moreover, with the diffusion of the webcams, it is also possible to verify the real conditions on the field without be physically in the place, gaining information and spotting every variation throughout time, about for example: traffic conditions, crowding and dislocation of law enforcement agents.

Using only public search engines it is possible to gain a clear and complete view on targets and those data can be used to plan an attack or to multiply the impact of the attack itself.

For example, a relatively new search engine that, in my opinion, could be very important in the future, is Shodan. This is a search engine devoted to the data retrieval on the SCADA (Supervisory Control And Data Acquisition) systems. On Shodan, everyone can find information ranging from HVAC (Heating, Ventilation, and Air Conditioning) systems of schools and hospital to public and private surveillance cameras to systems used by large industries to control their manufacturing processes. Moreover, these data can be sorted by country, brand, model, version, etc. using a specific set of queries provided by the site.

As it is easy to deduce, the information that can be gathered through Shodan by a terrorist group (but not only) could represent a major threat for all the industrialised countries, so I think that an initiative like Shodan has to be carefully scrutinised to clearly define the impact of the diffusion of these kind of information, mostly in the case of critical infrastructures. I think that also some relationships with the owner of the site should be established by governmental agencies devoted to the critical infrastructure protection to create a sort of alerting system in case of disclosure of sensitive information. In fact, though it is clear to me that every action toward a limitation of the use of Internet has to be avoided because of the dangers that are implied, this doesn’t mean that some mitigating measures haven’t to be adopted. For example a confidential tool that sends automatic warnings to some governmental agencies in case of the positive match for a keyword or a regular expression in the query results could be fundamental to mitigate the evil potentials of the use of such search engine.

Finally, OSINT and CYBERINT are made easier for everyone, including terrorists, by the general
habit to publish private and personal information on social networks. This new situation has produced a great mass of data that can be easily and efficiently examined in search of ways to exploit some personal and public vulnerabilities.

5.3 - Simulators and augmented reality

Our relationship with reality is profoundly changed with information technology and Internet, now we are used to interact with the physical objects with the awareness that, in case of need, we can immediately obtain information, help and manuals to guide us. Furthermore we know that, in many situations, we can easily find a simulator that can help us to gain confidence with the use of complex objects such as an aeroplane or a racing car.

Some real attacks had been prepared with the use of simulators and two cases hit the public opinion particularly: 9/11 and Oslo attacks.

In both cases it was proved in court that the terrorists had prepared their actions with the help of some simulators: in the 9/11 case they used a flight simulator to practice with the manoeuvre to hit towers and in the Oslo case Breivik used a holographic aiming device to develop target acquisition and to transform himself into a cold-blooded killer (Pidd, 2012).

Both cases represent another kind of evil use of innocuous tools by terrorist who showed the capacity of use the “lateral thinking” to achieve their evil goals.

Remaining on the malicious use of innocuous objects I found a new Internet device that, in my opinion, it is the perfect candidate to be the new helping tool in a big terrorist attack: Google Glass.

Google Glass is a device fundamentally based on augmented reality that according to Wikipedia definition is:

> “a live, direct or indirect, view of a physical, real-world environment whose elements are augmented (or supplemented) by computer-generated sensory input such as sound, video, graphics or GPS data.”

Wearing this device and giving vocal commands or touching the arm, it is possible:

- to see contextual information,
- to see the directions to reach a destination
- to send and receive messages and emails
- to shot a photo or record a video
- to perform Internet searches
- to interact with social networks, and
in the future, to recognize people obtaining also a set of information about them. Substantially, using this device, a tourist will be able to have information about the Colosseum just watching the ancient ruins but a terrorist commando will be guided through an unknown path to attack a target that will be automatically recognized in the moment it will appear.

![Figure 5 - A photo taken from the article "Google Buys Image and Gesture Recognition Company Viewdle" Ningauble, 2012](image)

It is also important noting that though at the moment there is a very limited diffusion of this device, the security of Google Glass has been recently violated finding a procedure to perform the so called “jailbreak” and gain root privileges (Gizmodo, 2013). This condition is very worrying because in this way it is possible for example to install unapproved software and modify the modes of use of hardware forcing the glasses to perform new actions or to be used in an unapproved new way.

But Google Glass are not unique, there are other HUD (Head-Up Display) on the market, one of these is particularly interesting for my reasoning: Brother-AIRScouter. This is a tool used in industry to help workers to perform complex tasks without a previous specific knowledge interacting with an expert and viewing contextual explanatory images.
This technology can open a new world of possibilities for a terrorist group that can gain an enormous power extending its possibilities to operate and to realising attacks.

So, at the moment my hypotheses are only a fantasy but I think that when these devices will be widespread in the public there will be someone ready to exploit their hidden evil side. Hence, a complete analysis of these scenarios is needed to be prepared to face the possible future emergencies.

6 - Cyberterrorism

In the following paragraphs I will analyse the complex problems deriving from the use of the Internet to directly attack a target by a terrorist group. It is important to remind (see par. 2.2) that to have a cyber terrorist attack there has to be a physical effect or, as described in the NATO definition, a sufficient destruction or disruption to generate fear or to intimidate a society.

Due to the bluriness on the definition I will start analysing some borderline phenomenons to arrive, at the end of the chapter, to the assessment of the risk of a specific cyber terrorist attack.

6.1 - Hacktivism or terrorism

Hacktivism is a term derived from the fusion of the word “hacking” and “activism” and it is used to indicate some kind of activities and attacks based on the use of Internet and finalised to the expression of a civil protest. Wikipedia define hacktivism as:
“the use of computers and computer networks to promote political ends, chiefly free speech, human rights, and information ethics. It is carried out under the premise that proper use of technology can produce results similar to those of conventional acts of protest, activism, and civil disobedience.”

But throughout time, this form of civil disobedience has assumed various forms and some of them are not close to the classical intended objectives. In particular, in the last years we saw a marked increase of some actions with questionable purposes, carried out with definitely illegal means. I’m mostly referring to some actions carried out by Anonymous, one of the major responsible for these crimes.

At the moment the most diffused forms of (so called) hacktivism actions are the following:

- Data breaches
- Distributed Denial of Service (DDoS)
- Defacements

Due to the nature of these methods, some doubts have arisen on the nature of these attacks and some governmental exponents classified them as real act of terrorism. The question is important because these kind of attacks have the potential to cause the “disruption to generate fear or to intimidate a society into an ideological goal.” referred in the NATO definition of cybercrime.

In the next two paragraphs I will analyse some cases just to explore the perimeter of this question and to find a plausible answer.

6.1.1 - Is DDoS always only a form of protest?

DDoS is one of the first form of protest used over the Internet. It was assimilated to a sit-in or a strike where many people occupying a public place stop the traffic or the access to a building. For a lot of time, the methods used to perform this kind of actions are representative of such form of protest. In fact, many people are requested to contact an Internet resource (or send an email) at a precise time and, if the virtual crowd was large enough, the DDoS was successful and the site (or the mail server) collapsed under the quantity of connections (or emails). Subsequently, the Internet websites became capable to stand all the connections generated by using simple browsers also in presence of a big amount of protesters, so specific pieces of software were written to multiply the number of connections generated by every protester. Throughout time many of these programs were released on the net but, recently, the program called “Low Orbit Ion Cannon” (LOIC), the one used by Anonymous, gained a very large popularity.

Armed with this tool, many hacktivists chose a target and started a coordinated action at the signal “Tango down”. These actions in Italy and in other countries were able to deny the access to many
important websites including governmental sites and sites owned by big companies.

But in Italy an interesting phenomenon have been started, after some arrests, the number of hacktivists became insufficient to perform successful operations also using LOIC, so some prominent elements in AnonItaly started to use botnets to achieve the result of blocking their Internet targets.

In my opinion, the use of botnets is a clear discriminant from a form of civil protest and a pure felony. In fact, when two or three people decide to impose their will through the use of an illegal tool, typically used by cybercriminals, there can be no form of excuse. This is a crime.

Furthermore, there is a clear example where this crime becomes so disruptive that the NATO definition of terrorism start to be applicable. This example is known as “Operation Ababil”.

Operation Ababil is a sequence of impressive DDoS attacks against U.S. financial sector started after the publication of the controversial video “The innocence of muslims” considered insulting by many muslims all over the world. A formation self proclaimed “Izz ad-Din al-Qassam Cyber Fighters” claimed responsibility for this series of attacks. This formation whose name is inspired by a famous Palestinian revolutionary also recall the name of the terrorist formation “Izz ad-Din al-Qassam Brigades” that has the role of Hamas armed force.

The peculiarity of these attacks was the use of web servers as enslaved elements of the botnet (Atias, 2013), in fact Incapsula team discovered a piece of malware hidden in a UK web server that was receiving commands from remote forcing it to flood some US bank sites.
Using this toolkit named “itsoknoproblembro” the hackers can utilise more connectivity than using a simple PC, moreover in some cases they use also the elasticity granted by cloud computing infrastructure to obtain even more power. Leveraging the web server vulnerabilities, these attacks have been as large as 60 Gbps with some peak of 100 Gbps.

The difficulties in managing these kind of attack was so important that American bank association requested the government intervention that was granted at the beginning of 2013 in a form of collaboration with NSA.

Finally, in recent times DDoS attacks showed the potential to disrupt normal way of life, in fact, in 2008 a massive DDoS attack put a strain on a small country with a heavy use of online technologies like Estonia. In that case, an active role of Russia was hypothesised but the potential to produce severe damages to a high-tech country remains very high also if a small group with access to large botnets is involved.
6.1.2 - Other forms of protest or other attacks?

Other recent attacks are very close to the NATO definition of cyberterrorism, for example in Israel there was a leakage of a massive number of credit cards by a hacker known as 0xOmar of the “group-xp” a political motivated Saudi Arab crew (Cavallini, 2012). 0xOmar published on Pastebin an announcement in which he pretended to have made available more than 400,000 israeli credit cards along with the necessary data to be used, promising to reach the number of 1 million cards in the future. In Israel there are roughly 6 million of credit cards and the supposed number of the leaked cards was enough to create a very complex problem with a lot of repercussions on the civil society. Luckily the real number of leaked cards was much lower than announced so the damages was limited but the statement of 0xOmar was interesting because clearly exposed a political motive and an intention to create disruption in the Israeli society, in fact he wrote:

"What's fun for us?
- Watching 400,000 people gathered in front of Israeli credit card companies and banks, complaining about cards and that they are stolen
- Watching Israeli banks shredding 400,000 credit cards and re-generate new cards (so costly, huh?)
- Watching people purchasing stuff for theirself using the cards and making Israeli credit cards untrustable in the world, like Nigerian credit cards
- and much more..."

This episode showed an “innovative” approach in which cybercrime techniques were used to create turbulences instead of illegal profits and represents a real episode that sits between hacktivism and cyberterrorism.

Furthermore, very recently, The International Organization of Securities Commissions (IOSCO), published the report “Cyber-crime, securities markets and systemic risk” (IOSCO-WFE, 2013) in which is written regarding the cybercrime attacks on exchanges:

“Attacks tend to be disruptive in nature (rather than aiming for immediate financial gain). The most common forms of attack reported in the survey are Denial of Service attacks and malicious code (viruses). These categories of attack were also reported as the most disruptive. Financial theft did not feature in any of the responses. This suggests a shift in motive for cyber-crime in securities markets, away from financial gain and towards more destabilizing aims. It also distinguishes cyber-crime in securities markets from traditional crimes against the financial sector e.g. fraud, theft.”

So, differently from which is stated by Pollit about the necessary conditions to spot a cyber terrorist attack, I think that the disruption condition invoked by NATO definition is more suitable to describe future attacks because the use of Internet tools open the possibilities to cause large damages and spread fear in the society without having recourse to real violence.
6.2 - Targets and scenarios

Analysing the threat of cyber terrorist attack, it is apparent that not all the possible target and the techniques are suitable, because the majority of the classical Internet attacks are focused on the realisation of a financial gain. But, should an attack be launched against systems and networks, the following would be at risk (Goodman, 2008):

- The Internet - with attacks against its infrastructure (e.g DNS)
- Embedded/real-time computing - with attacks against:
  - systems for air traffic control
  - SCADA systems
  - switching of telecommunications
  - bank teller machines
  - floodgates.
- Dedicated computing devices - with attacks against servers and desktop computers

I would like to highlight that an act of cyberterrorism can benefit from some advantages compared to usual kinetic attacks, in fact, on average, a cyber attack is facilitated in the reconnaissance step, can be launched remotely without a physical presence in the attacked place and can leverage the complexity of the modern infrastructures and the general diffusion of the vulnerabilities. Furthermore the investigations could be very difficult because of the presence of different legislations and because of the lacking of a widespread standard for forensic activities.

On the contrary, I think that there are also some disadvantages that have to be considered and among those the most important are:

- the difficulty in the attribution (anyone can claim, or deny, the responsibility for such an attack)
- these attacks are good for sabotage and denial of service but are not so “immediate” as a car bombing or a shooting
- the recovery time after a cyber attack can be faster than that needed after a physical attack.

Generally speaking the first scenario that comes to mind analysing a possible cyber attack is an attack against a national critical infrastructure (defined by the DHS as the assets, systems, and networks, whether physical or virtual, so vital to a country that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof) . In this scenario, SCADA systems play the major role and I will analyse in detail the impact and the characteristics of an attack against these systems in the next
Finally, it is worth noting that Internet itself is a significant target for an eventual attack. Particularly the Domain Name System (DNS) is prone to attacks that have the potential to disrupt the correct structure of Internet. Throughout time there have been attacks against this fundamental component of Internet and recently (June 2013) there were three seemingly coordinated attacks against three different DNS providers - DNSimple, easyDNS and TPP Wholesale -. These coordinated attacks highlight the disruptive potential of this kind of attacks (Constantin L., 2013). This wave of attacks was characterised by a DDoS approach that put the provider in a difficult position blocking its service supply. Most of these attacks share the same patterns and were fundamentally based on a DNS reflection technique against authoritative DNS servers, an uncommon technique that requires an extra effort by the attackers to determine precisely the mapping between the resource and the DNS server. If an attack like this is sufficiently large involving a significant number of DNS providers some real consequences are possible resulting in the impossibility to connect to Internet resources.

6.2.1 – Critical infrastructure and SCADA systems

As previously recalled, one of the main targets of terrorist attacks are critical infrastructure. These represent a suitable target for anyone who wants to cause large damages to a national state and their protection is a field in which modern countries have invested a lot of efforts and money. By their nature, critical infrastructure are vulnerable to many attacks both physical and cyber and often have also many interdependencies that link them with each other.

SCADA and ICS systems are the mean by which a layer of automation is put in current productive processes, critical infrastructure included. SCADA systems are used in real time monitoring and process control in many sectors such as the controlling pipeline flows for water, oil and gas, managing transporting systems, managing chemical, nuclear and electrical plants and many more. The problem is that SCADA systems are affected by a large number of vulnerabilities such as the following:

- Traditionally relied on security by obscurity
- Increasingly interconnected with private and public networks using common protocols
- Increasingly using COTS (Commercial Off-The-Shelf) products and sharing the same vulnerabilities, threats and challenges as other Internet connected networks.

There are a lot of evidences that these vulnerabilities are exploited by attackers in real episodes and there are many initiatives aimed at the reduction of their vulnerabilities. One of the most significant is ICS-CERT, the Industrial Control Systems Cyber Emergency Response Team (a team from
DHS) that works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among government and control systems owners, operators, and vendors. In a report of the Newsletter “ISC-CERT Monitor April-June 2013” there is an analysis of the cyber incidents in 2012 that highlight a general increase of such attacks (more than 200 reported attacks to critical infrastructures in the period October 1st 2012-May 2013) and an apparent focus against the energy sector that is the target of more than the half of the attacks. Again a direct financial gain is not an objective of the attackers.

![Figure 8 - The attack distribution among critical infrastructure sectors (ICS-CERT, 2013)](image)

Interestingly Ralph Langner, one of the most famous expert on SCADA security, gives an interpretation key for these kind of data. In fact, in 2012 he wrote for The New York Times:

“In cyberspace, the real threat comes from non-state actors against which military deterrence is powerless. It does not require the resources of a nation state to develop cyber weapons. I could achieve that by myself with just a handful of freelance experts. Any U.S. power plant, including nuclear, is much easier to cyberattack than the heavily guarded facilities in Iran. An attacker who is not interested in engaging in a long-term campaign with sophisticated disguise (which rogue player would be?) needs to invest only a tiny fraction of effort compared to Stuxnet.”

All these facts suggest that SCADA and ICS could be an ideal target for a cyber terrorist attack. In the following paragraphs I will analyse more closely a couple of specific sectors that are probably good candidates as target.

This analysis is so diffused and agreed that on 12 February 2013 President Obama issued an executive order titled “Improving Critical Infrastructure Cybersecurity” in which is stated that the cyber threat to critical infrastructure continues to grow and represents one of the most serious
national security challenges that has to be confronted. The core of this executive order is in my opinion the decision to sponsor a program to develop a “Cybersecurity Framework” that includes a set of standards, methodologies, procedures, and processes to align policy, business, and technological approaches in addressing cyber risks.

6.2.2 – Threat and vulnerabilities of the energy sector

Regarding the energy sector there is an interesting situation in which some providers are becoming aware that, to implement smart-grids and other cutting edge technologies that allow an easier and interactive way to communicate with energy meters, is necessary to put in place a secure environment. On the contrary there is a consolidated managing approach to maintain untouched critical systems in order to maintain the reliability of operational levels. Furthermore, the general consideration to the theme of cybersecurity within many critical infrastructure providers is very low because of some misleading beliefs such as the presence of the so called “air-gaps”, a physical separation between the operational internal network and the big Internet.

During my researches I had the opportunity to have proof of this situation. In fact exploring the Internet in search of information about the security of smart-meter I found many documents and sites that put in evidence some real vulnerabilities in operational systems. This situation added another concern: the easiness of finding sensitive information over the Internet. In the following I will treat two examples of my findings.

For the first example, during my researches I found a press release in which is stated that to counter the cyber threats, an electric power company has chosen the a specific site (with the indication of the precise physical address) as a center for cyber security. It is also said that, inside this center, this company reproduced an entire power station and simulated attacks of different types to see how systems react. The press released said that the response was not the best: "A computer in the network was able to control the valves that manage the regulation of the fuel to the turbine. At that point the company started a program to cope with these shortcomings with the result of a new and more robust security system that is routinely tested using a simulator.”

Using this information I could easily find a (sadly misconfigured) web server in which there are plenty of documents about this project. The majority of the documents are (semi) public but the fact to find all the material concentrated in one (vulnerable) web server represent a disturbing event.
This material could be very helpful for someone who is preparing an attack because it lays the groundwork for further and more exhaustive researches and gives a lot of indications about the
logic applied in the countermeasures.

Regarding the second example, searching for the presence of smart-meters in Internet, I found a web server (again poorly configured) that publish a complete management console in which are accessible all the real functioning parameters of a demo power station located in Belgium.

Figure 10 - A screenshot of the Home page of the management console published by Schneider Electric (2013)

Figure 11 - An example of the information that can be accessed using the Schneider Electric’s website (2013)

To give a simple example of the open source intelligence that can be done using just an insignificant part of these data, I want to mention the other result I found using the image of the plant on Google Image Search feature. The following article states that 52 jobs are at risk in that plant because of a project of internal reorganisation. This information can be very useful for a terrorist to infiltrate among disgruntled employees or to contact someone in order to obtain
sensitive information in exchange of money.

Figure 12 - The article about the possible job reduction in the Schneider Electric’s plant (2012)

All the exposed facts contribute to depict a worrying situation in which the possibility to gain the pieces of information necessary to plan and execute an attack in the energy sector against a critical infrastructure and its managing components is real and effective.

6.2.3 – Are the transportation systems really at risk?

Another sector that has been repeatedly reported to be at risk of cyber attack is transportation systems. Many researchers are concordant in considering the computerised systems that manage airplanes, trains, metro and even ships are usually not updated and with many unresolved vulnerabilities. This fact is mainly due to the necessity for these systems to be always up and
running but having enormous difficulties to set up a clone system in which testing the patches and the fixes prior to deploy them in the operational system.

So the most probable situation is that these systems are carefully tweaked once before passing the first test and then remain in the same state for all their operational life. Unfortunately this choice causes the continuous widening of the attack surface because of the discovery of new vulnerabilities in the operating systems and in the specific application. A manna for all kind of attackers, cyber-terrorist included.

Among others, a real case happened in Poland in 2008 (Baker G., 2008) shows the hidden potential of these kind of attack. A Poland 14 schoolboy in Lodz, after a studying and discovering time was able to prepare a sort of infrared remote control that force the Lodz tram system track points to change position causing a deviation of the arriving trams. He probably underestimates the power in his hands and the potential consequences of his acts so, using his remote control, he caused the derailment of four trams and many other problems. 12 people were injured and just for a lucky case nobody died.

Anyone can easily imagine the power of such remote control if in possession of a group of terrorists.

Changing scenery, there is a recent study about the cyber vulnerabilities of the U.S. port facilities (Kramek J. 2013) that highlights some problems in the management system of the U.S. port. For example, Commander Kramek highlights that the Port of Houston presents a high reliance on networked systems for their terminal operations and security, but the IT department neither has done a cyber security vulnerability assessment on its systems nor has developed a cyber security incident response plan. Sadly, Commander Kramek wrote:

“If PHA were the victim of a cyber attack, it does not view any federal government agency as a partner. Rather, it would rely upon in-house IT staff to manage any response.“

But in other parts the Kramek report is definitely less convincing. For example, when he affirms more than once time that:

“In the midst of this lacuna of authority is a sobering fact: according to the most recent National Intelligence Estimate (NIE) the next terrorist attack on U.S. Critical Infrastructure and Key Resources (CIKR) is just as likely to be a cyber attack as a kinetic attack”

citing an article published on the Washington Post (Nakashima E. 2013) that treats only the topic of cyber espionage without writing the word “terrorism” even once. Moreover I couldn’t find another reference or an independent link that supports Kramek’s assertion.
Citing this report I want to show how much confusion is around these themes and how it is easy to leap to not verified conclusion in this field in which the word “cyber” is put before everything to create new scenarios and, sometimes, to disseminate FUD (Fear, Uncertainty and Doubt).

6.3 – New opportunities for the cyber-terrorists

As I stated in the previous chapters a physical effect of some kind is necessary to be able to set a cyber attack as cyberterrorism, alternatively, a disruption of a critical system could be classified as such but it is undeniable that the new cyber-world open up new possibilities for criminals and especially for terrorists creating a blurred territory in which cyber crime and terrorism will mesh together. In the next paragraphs I will analyse the new major opportunities that in my judgement could be more relevant in the next future.

6.3.1 - Crimeware: exploit kit, botnet e financial malware

As I mentioned before, citing the Tsouli case, cyber criminal activities can be a very effective form of funding terrorist groups but at the moment I cannot find a real case in which some terrorist group used directly crimeware (financial malware aimed to commit crimes). At the moment there isn’t a significant collaboration between underground groups that sell financial malware and terrorist. In my opinion there are the basis for a change in this situation. History offers plenty of examples in which terrorists mimicked the behaviour of criminal groups in order to finance their projects. In Italy for example, during the 70’s it exploded the phenomenon of the so called “proletarian expropriations”, real armed robberies carried out by terrorists to finance the operations of small and medium cells.

I think that, with a high degree of likelihood, this kind of situation will be replicated in cyberspace and we will be witnesses to the birth of this new form cybercrime.

When there will be a well established use of the crimeware such as Zeus or Citadel by the terrorist groups there will be the conditions for new “creative” use of this instruments. Hypothesizing a transport of the up-to-date uses of the crimeware in a terrorist field I can imagine some scenarios such as the following:

- the use of botnets to mail a massive number of “spam” emails with threatening messages during the execution of a kinetic terrorist attack to both conduct a disinformation campaign or to diffuse malware
- the use of the MITB (Man-in-the-browser) features typical of Zeus or of SpyEye to conduct or support psyops (e.g. conjuring up false and scary news while a victim used an infected PC to surf news websites)
- the use of the ransomware techniques to cripple PCs and to scare population
In this view, the use of crimeware would be an essential part of the attack strategy giving real advantages to terrorist. In this sense we can describe it as cyber terrorism though the cyber component doesn’t cause directly the destruction because it would be impossible to achieve the final effect of the attack without using it.

6.3.2 - Cyberweapons: the future of terrorist attacks?

Very recently Stefano Mele, a lawyer expert of cybersecurity and cyber intelligence, published a study titled: "Cyber-weapons: legal and strategic aspects” in which is proposed the following definition for a cyberweapon:

“A part of equipment, a device or any set of computer instructions used in a conflict among actors, both national and non-national, with the purpose of causing, even indirectly, a physical damage to equipment or people, or rather of sabotaging or damaging in a direct way the information systems of a sensitive target of the attacked subject.“

After Stuxnet, the world discovered that a cyberweapon is something real and effective. With this piece of malicious code, in fact, the U.S. (with the probable collaboration of some other national government) retarded the Iranian nuclear program by sabotaging the uranium enrichment process. For the first time in history a piece of code was used to create a physical damage (the enrichment centrifuges produced something different from the expected uranium and were prone to severe damages) to an enemy infrastructure. This was a game changer because showed to the world that a new a way to attack an enemy was possible, with a lot of advantages such as the following:

- the attack is remote, no forces have to be deployed directly on the field
- the attack is deniable, no one can clearly indicate the culprit of such an attack
- the attack surface is huge, no one can defend properly all infrastructure

All these considerations don’t pass unnoticed to the state and non-state actors.

During summer 2012 a malware was released in the Saudi Aramco’s network causing a lot of damages. In particular this malware, called Shamoon (or Wiper) by the antivirus vendors, was built to erase the information in hard disk, Master-Boot-Record included. This so exhaustive cancellation produced more than 30,000 PC completely unusable also after attempts to reinstall the operative system. All the infected machine have to be replaced. Probably the real objective of this attack was the crude oil production, but also with the reported results the attack was a significant problem to solve for the state company. Regarding the attribution, as recalled before, it is very difficult to have enough information to spot the real responsible for an attack, in this case, even if some researcher indicated Iran as a final sponsor of the attack, there was a plausible claiming of the responsibility for the attack by an islamist group (Bumgarner J., 2013).
It is now easy to foresee what an attack like this one could imply for a power provider, for a telecommunication provider or for a critical infrastructure. This could be a disaster capable to disrupt the normal life of a country.

Moreover, if we analyse the use of a cyberweapon by a terrorist group we find that this kind of actor is in the best position to use such a weapon in fact, one of the major problems with the use of cyber weapon is the difficulty to limit the effect to a single target without “side effects” and collateral damages and this can be a big limitation for a military entity or for a state actor but not for a terrorist group.

Hence, at the moment, the most important difficulties to overcome for a terrorist group who wants to attack a target using a cyberweapon are:

- to gather all the pieces of the information needed to develop and use the weapon
- to find the right vulnerability/vulnerabilities to exploit during the attack
- to find people who has the knowledge to develop such a weapon

Certainly big problems but not impossible to get over.

6.3.3 - SWATing and TDoS

Looking at the present and at the near future we find a lot of vulnerabilities in the telecommunication field and criminals are quickly learning how to leverage them to make money. Terrorists are in the position to include these new attack techniques in their attacks creating blended threats that can mix “old style” attacks and new cyberattacks.

Two example of this scenario are the so called SWATing and TDoS.

SWATing (or swatting) is defined by Wikipedia (Wikipedia, 2013) as the tricking of any emergency service into dispatching an emergency response (deployment of bomb squads, SWAT units and other police units and the concurrent evacuations of private and public buildings) based on the false report of an on-going critical incident. Caller ID spoofing and phone phreaking techniques are used to trick 911 systems so the caller typically places a 911 call using a spoofed phone number with the goal of tricking emergency authorities into responding to an address with a SWAT team to an emergency which doesn't exist. This practice can give a significant contribution in causing massive disruption during a terrorist attack by deploying the police and other civic resources such as ambulances and fire departments in wrong places.

TDoS (Telephony Denial of Service) is simply the transposition of a DoS attack in world of telephony and in the last couple of years is growing fast gaining a place in the ranking of most worrisome attacks. Until now it has been used to extort money from some public and private entities in a classic ransom scheme: if you don’t pay us we can block your phone damaging your business and your image, but the potential use in case of a terroristic attack is enormous. Just think
someone can deny the telephone emergency service during an attack or isolate the attacked building to comprehend the potential of this technique as impact multiplier. Finally, the increasing use of VoIP (Voice over IP) as telephony solution has broadened the possibility of realising such an attack.

6.4 – Assessing the risk of such an event

One of the key points to analyse a phenomenon like cyberterrorism is to correctly evaluate the risk bound to the realisation of such an event. Since using a complete risk assessment methodology is beyond the scope of this research, in order to produce a reliable evaluation, I took my cue from the national risk assessment methodologies just because they are tweaked precisely to assess these kind of events. In particular, I used two methodologies as references: the UK National Security Risk Assessment (NSRA) as described in “The National Security Strategy” (2010) and the National Security and Safety Method (NSSM) of the Netherlands (Bergmans H. et al., 2009). With the support of these two methodologies I adjusted a simplified qualitative approach to evaluate the risk of a cyber terrorist attack, assessing the possible impact and its relative likelihood over a 5 years horizon. The plausible worst case scenario of the threat posed by a cyber terrorist attack was scored in terms of its likelihood and its potential impact.

6.4.1 – Description of the risk assessing method

To evaluate the impact I used a simplification of the table proposed in the NSSM document. In the following table there are the criteria that I judged relevant for the present case

<table>
<thead>
<tr>
<th>Vital interest</th>
<th>Impact criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Physical security</td>
<td>1.1 Fatalities,&lt;br&gt;1.2 Seriously injured and chronically ill,&lt;br&gt;1.3 Physical suffering (lack of basic necessities of life)</td>
</tr>
<tr>
<td>2. Economic security</td>
<td>2.1 Costs</td>
</tr>
<tr>
<td>3. Social and political stability</td>
<td>3.1 Disruption to everyday life,&lt;br&gt;3.2 Violation of the democratic system,&lt;br&gt;3.3 Social/Psychological impact</td>
</tr>
</tbody>
</table>

For each of the seven listed criteria, the impact is rendered measurable by using five categories classified as follows:

A = Limited consequences
B = Substantial consequences

45
C = Serious consequences
D = Very serious consequences
E = Catastrophic consequences

To combine the obtained values and calculate the final value for the impact I decided to adopt a linear value function (where the distance between the labels is equal and E again has the value 1 and the interval [0..1] can therefore be divided into five equal parts: X = 0, A = 1/5, B = 2/5, C = 3/5, D = 4/5, E = 5/5) and then calculate the average value.

Regarding the likelihood, this is primarily calculated evaluating two factors:

- the likelihood that a terrorist group has the capabilities and intentions for this specific threat
- the likelihood that the vulnerabilities in the targets makes the attack successful

The assessment of the likelihood of a specific threat scenario leads to the determination of a category (A, B, C, D, E). If vulnerability is evaluated as high (for ICT Systems high vulnerability derives from the presence of one or more of the following conditions: no information policy, large number of Internet accesses to systems, limited/no policy and compliance regarding anti-virus protection, firewalls, passwords, no ISO 27001 certification, no disaster recovery plan, incompetent staff members or understaffing) the category is increased by a unit (e.g. C becomes D). In the following image, modified from a scheme published in the NSSM document, there are the passages to evaluate the likelihood of a malicious event.

Figure 13 - A modification of the “Determination of the likelihood” taken from NSSM document
6.4.2 – The cyber terrorist scenario

One of the major objections against the hypothesis of a cyber terrorist attack is that, in the short term, there isn’t a terrorist group that can develop the necessary skills and competence to plan and conduct such an attack. My opinion is that there is a possible case in which this objection is irrelevant. This case is based on the action of a lone actor who already possess the skill and the competence to plan and conduct a cyber terrorist attack. This lone actor could be an insider, someone who works for critical infrastructure and is in the position to have the knowledge and the opportunity to carry out the attack. In support of this hypothesis there is the recalled fact that senior Al Qaeda figures have urged Muslims in the West to conduct attacks without training or direction from established groups. Such lone terrorists are inherently unpredictable and their plots are difficult to detect. Al Qaeda may consider these attacks to attract considerable media attention. This situation is even more complicated by the fact that attack surface is continuously in expansion, in fact while cyberspace provides opportunities that cannot be missed, the risks emanating from growing dependence on it are huge.

The following scenario is a modification of the “Malicious long-lasting electric power cuts” inserted in the “Scenarios National Risk Assessment 2008/2009” (National Safety and Security, 2009).

**Description**

A second generation immigrant employee, a skilled IT engineer working for a major energy provider, was in touch with some radical elements in his country of origin. He was determined to conduct an attack aimed to cut off the electricity for a long period of time to protest against the imperialistic politics of his country. He set up a hidden routine that at a given time sends commands to various SCADA systems in the power station causing the overcharge of the grid and finally the explosion of the turbines. The entire power plant was heavily affected by damages and there are also some casualties between the employees. The electricity is cut off in a large part of the country. Daily life grinds to a halt on a wintry morning. Many people are stranded in the morning rush hour because public transport by train comes to a halt and traffic lights fail. In people's homes and offices, radio and TV are no longer working; computers (and Internet connections) fail; fixed and mobile telephony are disrupted; the heating doesn't work anymore; cash machines don't work; production processes are stopped; home dialysis machines are no longer working; etc.
However, during the morning, reports start coming in that a terrorist attack by a jihadi lone terrorist has caused the explosion of one of the largest energy production site in the country. The electricity industry indicates that the infrastructure has been hit very hard. There have been a number of fatalities. Repairs to the electricity supply infrastructure in the affected area will take between a few days and a few weeks. The electricity companies will have to show improvisation to deal with the situation because this scenario wasn’t taken in account as possible. A few possibilities are feedback to the grid by combined heat and power systems in large industries and the installation of gas turbines. This will make a limited amount of electricity available. After approximately three to four weeks, electricity supplies will be back to normal. However, the network remains vulnerable, leading to possible blackouts during the continued build-up towards the pre-attack situation. Complete recovery of the infrastructure could take more than one month.

6.4.3 – The results of the risk assessment

Since a complete analysis is beyond the scope of the present research, the following results are directly derived from the analysis in the “Malicious long-lasting electric power cuts” inserted in the “Scenarios National Risk Assessment 2008/2009” (National Safety and Security, 2009).

Likelihood of the event

The scenario is based on malicious acts. The likelihood is rated as unlikely (class B). There is no concrete indication and the event is deemed somewhat credible. Due to the relatively high vulnerability of the sector and the effective incidence of lone terrorists attacks, the ultimate likelihood is rated as 'possible' (class C).

Impact

1.1 Fatalities

As direct consequence of the blast there were some casualties in the plant moreover a few fatalities can be expected on the roads and at home, among patients who are dependent on medical equipment. Additional people may die, compared with the normal winter deaths due to the lack of heating. In particular, this relates to the elderly and people who live in social isolation. There will also be victims of rioting and looting as well as in the chaos of evacuation. Premature deaths cannot be ruled out, but the assessment is that there will be few victims in the longer term. No empirical data is available. A few dozen fatalities are deemed the most likely by the NSSM analysis. The upper limit of the possible casualties is valued in the few hundred. (B)

1.2 Seriously injured and chronically ill

People could be injured in the explosion of plant during the attack, then many injured are possible
both in riots and in road traffic accidents. The number of seriously injured will probably be more than 100, but a higher number cannot be ruled out. (B)

1.3 Physical suffering (lack of basic necessities of life)
In the first moments after the attack all citizens in the country. All people in the directly affected area will be deprived of electricity for at least a month. Some of them will have no electricity for a long period of time (more than a week) and some will experience many brownouts and blackouts for more than a month. Due to the power blackout, some people will not have drinking water (country-houses and flats higher than the third floor) or any heating. (D)

2.1 Costs
There is great economic damage directly resulting from the explosion of the plant and indirectly electricity being cut off. Loss of added value, spoiled food, extra security costs, repair costs, and reduced income from tourism and business travel. An appraisal of the total costs in that first month will be in the rage of billions of Euros. (E)

3.1 Disruption to everyday life
During the blackout subsequent to the attack the normal life in the country will be impossible. In the following days, due to the power failures, many people in the affected area will not be in a position to conduct the usual life: to work, to go to school, to use ICT, to use ATMs or cards, to do essential shopping, to refuel vehicles. Many commercial businesses and malls will be closed. A large part of the entire population will suffer some consequence affecting its everyday life. (D)

3.2 Violation of the democratic system
The power being cut off will impair the functioning of political representation and public administration in the affected area. (B)

3.3 Social/Psychological impact
As a direct consequence of the terrorist attack and the long duration of the ensuing power failure, a large number of people will exhibit public anxiety and anger about further attacks. This includes: avoiding public places and public transport, staying at home, no longer flying, leaving the affected area, looting and hoarding, taking money out of the bank. In addition, a group of people will stigmatise immigrants and Muslims, because the attack was carried out by a second generation immigrant belonging to an Islamist group. Many protest against the government because of the impreparation in the prevention of such an attack and because the restoration of the electricity supply is taking a long time. (D)

<table>
<thead>
<tr>
<th></th>
<th>1.1</th>
<th>1.2</th>
<th>1.3</th>
<th>2.1</th>
<th>3.1</th>
<th>3.2</th>
<th>3.3</th>
<th>Average Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>B</td>
<td>D</td>
<td>E</td>
<td>D</td>
<td>B</td>
<td>D</td>
<td>C/D</td>
</tr>
</tbody>
</table>
In order to visualise the risk associated with this attack I added this event in a graph published in the NSSM document.

Figure 14 - A modification of the “Risk Diagram” taken from NSSM document with the insertion of the Cyber terrorist scenario.

Just as a final notation I would like to cite the Priority Risks emerging from the UK NSRA:

“The National Security Council judged that currently – and for the next five years – tackling the risks from terrorism, cyber attack, international military crises, and major accidents or natural hazards should be our highest priority objectives.”
I judge of some interest that the first two risks are terrorism and cyber attacks but an intersection between them is not considered at all. Perhaps a bit of close examination could be appropriate.

7 - Conclusion

Historically, terrorist groups have been able to leverage the benefits offered by Internet in many ways:

- as a main communication tool, bypassing the filter of the journalists of the traditional media;
- as a way to communicate securely and secretly to solve the problem of maintaining the necessary coordination between scattered and independent cells;
- as a mean to share know-how and directives;
- as a tool to facilitate the collection and the transfer of the money to fund the operations on the field.

Now, a new way to use Internet seems possible, the use of Internet as a weapon to directly conduct real attacks. From a terrorist point of view there are many difficulties to carry out this task but the extension of the attack surface and the possibilities to hit targets otherwise out of reach represent a strong incentive to pursue this objective. Furthermore the strategy adopted by many terrorist group to privilege action based on lone actors or lone terrorists can be a way to circumvent some of the difficulties. In fact, if a cyberattack is planned and carried out by an insider, that is someone who is already in possession of the necessary skills and he is in a position to gather the necessary information, all the difficulties could be overcome.

Finally the extensive use of SCADA systems to automate processes and to control industrial and
power sites can open new possibilities of massive destruction, very tempting for a terrorist.

Given these assumptions, one or more cyberattacks carried out by terrorist groups are possible in the next future, opening a new era in the fatal history of terrorism.

As security researchers, we will have the duty to analyse all the possibilities and try to foresee the most likely scenarios in order to give the chance to decision makers to adopt the right decisions to fight terrorism in every form in which it will turn up.
Bibliography


Brother (2011) “AiRScouter” see-through type head-mounted display of Brother” Youtube http://www.youtube.com/watch?v=5rtxz1P2Ogw#at=17 Retrieved 2013-06-20


g-finaldef-nietopgemaakt.pdf Retrieved 2013-07-31

Retrieved 2013-05-28


Pidd. H, (2012) “Anders Behring Breivik spent years training and plotting for massacre” and  
“Anders Breivik 'trained' for shooting attacks by playing Call of Duty” The Guardian  
http://www.guardian.co.uk/world/2012/aug/24/anders-behring-breivik-profile-oslo?INTCMP=SRCH and  

Pollit M, “Cyberterrorism – Fact or Fancy?” FBI Laboratory  


Schneier B. (2009) “Terrorists may use Google Earth, but fear is no reason to ban it” The Guardian,  

Retrieved 2013-06-08


TrueCrypt “The Hidden Volume” official website http://www.truecrypt.org/docs/hidden-volume

56
Retrieved 2013-06-19


