Defining the threat: what cyber terrorism means today and what it could mean tomorrow

Gianluca Riglietti
The Business Continuity Institute
Reading, United Kingdom

Keywords
Cyber terrorism, social media, propaganda, terrorism, cyber weapon, Internet of Things

Abstract
As terrorist organizations have become more resourceful and articulate, they have started to utilise the Internet to expand and improve their operations. This is often referred to as cyber terrorism. While several attempts have been made to clearly define this phenomenon, there is no consensus on one international definition. Looking at the literature so far, this paper tries to highlight those characteristics that best describe cyber terrorism today, while also exploring its possible future developments. In order to maintain a hands-on approach, the analysis will provide real life examples from terrorist organizations such as the Islamic State (IS) or the Taliban that are strongly involved in cyber activities.

When it comes to defining cyber terrorism, there is no international agreement. Different sources have described it in different ways, trying to strike a balance between the virtual and physical factors included in it. This combination of old and new has divided experts on the matter, whilst those deemed terrorists have developed increasingly sophisticated cyber skills.

The aim of this paper is to compare different definitions of cyber terrorism, trying to find the most appropriate one for current and future threats. In order to do this, it will employ a literature review, providing also an observation ofreal life instances of what is considered as cyber terrorism. The analysis will also examine how this phenomenon might evolve in the future, in line with upcoming technologies and the cyber skills of terrorist groups.

Accordingly, there will be three main sections. The first one will discuss the definition of cyber terrorism, while the second and third ones will respectively deal with present and future threats.

Defining and describing cyber terrorism.

In an age of increasing online attacks and terrorist activity, the fear of cyber terrorism has come to exist. The term was coined in the 1980s by Barry Collin, who pointed out how the physical and virtual words were starting to merge in relation to some aspects of terrorism (FBI, 2011). The term has spread widely and quickly since its creation, with law enforcement, academics and media using it to refer to various instances and not always in an accurate way. For instance, both attacks against IT infrastructure and online bullying have been regarded as cyber terror, while perhaps the latter should be more correctly defined as cyber crime. Confusion usually derives from the fact that methods used by cyber criminals and cyber terrorists can be the same, although the goals might be different (Krasavin).

Some experts have expressed scepticism towards the term itself, describing it as "useless", and saying that the cyber space is nothing but another means for terrorist activity. In this respect, the lack of a clear and unified stance by governments towards the issue is preventing the discussion from clarifying the meaning of cyber terrorism. Conflicting interests have led to a stalemate on an international level, which does not allow for a development of new up-to-date measures to identify this threat appropriately (Baranetsk, 2009).

Specialists have highlighted the importance of context when drawing a difference between cyber terrorism and cyber crime. Although similar hacking techniques might be used by both terrorists and criminals, only if the perpetrators aim at causing physical damage for political motives it is possible to talk about terrorism. Differently, cyber crime refers to any givenillicit activity in the web (InfoSec, 2012).

Adding to this discussion, a report from Symantec (2003) named "Cyberterrorism?" underlines how the Internet can enhance the potential of a terrorist organization, enlarging its capacity for sustainment and the accomplishment of its goals. For instance, terrorists can expand their influence to wider geographical areas thanks to online communication (email, chats, etc.), while also being able to recruit and finance themselves more easily. Their propaganda can be boosted too, with potential new members being able to read all about a terrorist organization, become familiar with their methods and act in a deregulated way. These are sometimes referred to as "lone wolves", as they usually have little if any direct connection wit the terrorist group itself. These individuals have a high potential for disruption and are very hard to catch, since they might never be in actual contact with another member of the organization while plotting and carrying out the attack. The report also introduces the concept of pure cyber terrorism, which refers to attacks that have no physical involvement at all but can still cause damage for terrorist purposes. It is still hard to say what this entirely virtual terrorism might look like, and while this is certainly a topic worth exploring in the future, physical elements should remain part of the analysis for now (Gordon, Ford).

In this regard, Denning (2000) stresses that there is little evidence of purely virtual attacks that can be classified as cyber terrorism, since these groups are mainly using the Internet to spread their message and carry out their activities on the ground. In order to examine the issue, she quotes a 1997 definition from an FBI special agent that classifies cyber terrorism as the "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents" (Denning, 2000, as in Pollitt, 1997). According to this definition, most of the terrorist activities seen on the web at the time of the article did not fit into the category, being considered only a future scenario (Denning, 2000).

While this description might have been accurate in the early 2000s, the perception of cyber terrorism has evolved over the years (although not necessarily in a clearer way). The FBI itself has changed the wording several times (Baranetsky, 2009), and today the Bureau is quoting definitions that embrace larger activities other than the sole targeting of IT infrastructure. For instance, they cite research from the Centre for Strategic and International Studies, defining cyber terrorism as "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information" (Tafoya, 2011, as in Lewis, 2010).

Furthering this more inclusive idea of cyber terrorism, Awan (2014) compares two different perspectives, the first one considering the computer as the main or exclusive weapon and the second one regarding it as a tool to a larger plot (e.g. radicalisation, guidelines on how to build explosives). The author states that most of the terrorist acts involving the Internet fit the second hypothesis better than the first one. Evidence in support of attacks that caused severe loss of life or serious physical damage through the sole use of a computer is still limited. Nonetheless, this does not exclude the possibility that in the future, as terrorists acquire more sophisticated knowledge, a machine could be used as the only means to a physically disruptive attack (Awan, 2010).

However, for the time being, when dealing with the threat of cyber terrorism, it would be perhaps more accurate to refer to it as the malicious use of the Internet by terrorists. The United Nations Office for Drug and Crime (UNODC) (2012) divides this in six main areas, namely propaganda, financing, training, planning, execution and cyber attacks. These categories are briefly discussed below:

a. Propaganda:Online platforms have increased dramatically the potential for publicity of terrorist groups, spreading their ideas via any virtual possible means (videos, audio messages, chats, social networks etc.). This also comprehends activities of incitement, recruitment and radicalisation of new affiliates.
b. Financing:The search for financial resourcescan be conducted through several channels. These comprise direct approach, e-commerce, online payment systems and the use of apparently legitimate organizations. The possibility of having websites dedicated to these activities helps terrorists in facilitating the flow of money with lower detection rates.
c. Training: Over time terrorist groups have developed several ways to train new recruits through the Internet. This involves sharing materials on how to produce rudimental weapons and how to carry out an attack. Online training platforms can boost an organization's reach-out by a great deal, leading to the creation of well-established journals such as Al-Qaida's Inspire.
d. Planning: Internet resources have also had the effect of making it easier to plan an attack. Gathering intelligence on a given target is easier today thanks to the vast amount of open source information that is available, from social media to geographical information programmes (e.g. Google earth). Furthermore, there is the possibility for plotters to use encryption in order for them not to be detected.
e. Execution: All of the above can contribute to the final execution of the attack, with the additional advantage that the parties involved in the preparation of the plot but not in the execution itself will be much harder to catch if they have used the right precautions while sharing information or conducting background research (among others).
f. Cyber attacks: These are also mentioned by UNODC, although they are addressed as topic for future research rather than in the immediate discussion.

This section has aimed at finding a definition for cyber terrorism. It appears that since there is no agreement on the matter it would be more correct to talk about the malicious use of the Internet by terrorists. The idea of the author, in agreement with Awan, is that current examples of cyber terrorism have more to do with propaganda, recruitment, planning and similar activities rather than the exclusive use of a computer as a weapon. In addition, new online platforms also tend to offer terrorists higher levels of publicity, which help them spread their message more quickly and effectively (Majoran, 2014). Nonetheless, the future is open to new threats conditional to the acquisition of further knowledge from terrorist actors. Hence, the next two sections will examine current examples and future possibilities of the interaction between terrorists and the Internet, to prove how this hypothesis matches with reality.

Cyber terrorism: what it looks like today

According to data from the Global Terrorism Index, Statista and *The Economist*, the following countries have been the most affected by terrorism in recent years: Syria, Iraq, Nigeria, Afghanistan and Pakistan. The most active groups in the region, in terms of terrorist attacks carried out, have been the Islamic State[1] (IS), Boko Haram, the Taliban, and the Fulani militants (Global terrorism index, 2015, The Economist, 2015).Therefore it is safe to say that these are probably if not definitely the most dangerous terrorist organizations in the world at the moment. Out of these four groups, the Taliban and IS seem to be by far the most advanced in terms of exploiting the Internet, and therefore they will be the centre of the analysis for this section of the paper.

[1] It should be noted that the Islamic State is also sometimes referred to as *Daesh*, ISIS or ISIL.

The Taliban share a vast number of information on the Internet, from audio and video material to news and religious speeches. They do this through several websites they keep running despite a fierce online fight from domestic and international powers, which try to shut them down with limited success. They communicate in five different languages, both local (Farsi, Pashto, Dari Urdu) and international (English, Arabic). In addition, they make an extensive use of social media, email and online forums to communicate with the public and possibly attract more recruits (Hairan, 2011).

The group uses accounts on websites such as Facebook, Twitter and YouTube to carry out propaganda but also to attract the attention of possible financers and get in touch with them. These accounts can reach thousands of followers, showing both religious messages and more practical instructions (e.g. on how to build explosives) (Gwakh, 2011).The Taliban have gone as far as to create an app for the Google store that users could download to get access to the latest news and speeches from the group. While this was removed from Google two days after its launch, it is a worrying sign of the interaction between terrorist organizations and new online technologies (Hern, 2016).

On the other hand, there are no recorded cyber attacks from the Taliban that led to physical disruption or loss of life using a computer as the only weapon. Rather, they exploit the Internet to grow, expand and coordinate attacks, mixing the cyber and physical elements. This fits more into the list provided by UNODC and Awan's argument than the views of Denning and Pollitt that tend to view cyber terrorism as a purely virtual issue. Nevertheless, it would be unwise to rule out the development of new techniques, including only computer based ones, from the Taliban, as they may want to step up their game to avoid losing ground to IS.

Indeed, it is no secret that IS has been flexing its muscles in the cyber field too. They referred to themselves as the "Cyber Caliphate", through messages shown by media affiliated to the group. One of their major successes was to unite different pro-jihadi hacking groups under one umbrella organization, the so called United Cyber Caliphate, which included the Sons Caliphate Army, the Caliphate Cyber Army, and the Kalashnikov E-Security Team. IS has been very successful at producing its own propaganda through social media and other online platforms, creating also their own forums and websites. Moreover, they managed to carry out a series of cyber attacks, exclusively computer-based, which in one instance even led to the disclosure of private information regarding US government officials, from private conversations to work and email addresses. Such strong presence in the various layers of the web (surface, deep, dark) has also helped IS get the attention of like-minded skilful hackers. This has strengthened their cyber army, even though the group is not directing its recruitment campaigns exclusively at cyber experts(Alkhouri, Kassirer, & Nixon, 2016). On a different note, terrorist organizations including IS have used hacking techniques to fund their activities in the past, revealing once again how these groups mainly use the Internet to further their plans. Whether they sent the stolen money to Syria and Iraq or they kept it for plots in the West, methods such as spear phishing, social engineering and malicious software were pivotal to raise funds(Williams, 2015).Yet, there is no consensus by the intelligence community on the current level of danger posed by IS in the cyber space. Some claim that jihadi hackers might actually be able to hack into critical national infrastructures and cause severe damages, especially since they have already started to try compromising different US power plants. Contrarily, experts argue that in spite of their tenacity IS perpetrators have been lacking the skills to constitute serious dangers, producing rather unsophisticated attacks (InfoSec, 2016).

IS appears to have developed broader cyber capabilities than the Taliban, although both groups appear very active in terms of propaganda, financing, training, planning, and execution of attacks. When the Internet is used to coordinate and organize physical attacks, these two groups have frightening potential and expertise, but they seem to be not mature enough to develop deadly cyber attacks. Once again, it is reasonable to assume that the current threat is posed by the malicious use of the Internet by terrorist actors rather than cyber attacks with no physical involvement whatsoever. This latter type of threat might take place in the future though, as terrorists build increasing cyber knowledge.

Cyber terrorism: what it might look like tomorrow

Thus far, this paper has provided a description of what cyber terrorism looks like today and compared it with current events to justify such a claim. In addition, it has opened the possibility for increased sophistication of cyber terrorism in the future, including increasingly computer-based approaches. While dealing with terrorism in its various forms might appear to some as an issue exclusively for the security services, this is actually a significant concern for private companies too. According to research, the top two disruptions that concern several industry sectors (e.g. financial, professional, defence)in the future are cyber attacks and data breach, with terrorism being number four (Alcantara, Riglietti, 2016). In this perspective, it makes sense to see what these could look like in the long term if combined under the umbrella of cyber terrorism.

According to Robert Hannigan, Director of GCHQ, the increasing blending of physical and cyber devices in regular activities could pose a danger as more and more objects become hackable. This happens as the so called Internet-of-Things grows in popularity. Mr. Hannigan was quoted saying that “We’re not quite there yet, but as the world becomes ever more connected that will become a greater risk” (Bodkin, 2016).

On the other hand, a report from CSIS backs the point that IoT technologies create higher vulnerability but it regards them as more suitable for crime rather than terrorism, the point being that IoT is more likely to be exploited for economic gain than physical disruption. This will also depend on the level of autonomy that is given to IoT devices, such as cars or airplanes. If these were to be governed solely by a machine, then the potential for physical disruption in the case of a hack would be extremely high. Conversely, if these high-tech machines are built allowing humans to overrule them in case of emergency, risks will probably decrease (Lewis, 2016).

Threats have already being developed to undermine IoT appliances, such as “worms”, which exploit lacks of updates to compromise a system, allowing the attacker to take control of several devices, such as cameras or computers, leaving the victim unaware (O’Brien, 2014). To get a sense of the potential for disruption of hacking IoT technologies, it might be useful to know that at present there are nearly 23 billion IoT connected devices, which are forecasted to more than double up to 50 billion by 2020 (Statista, 2016). This appears not to constitute a serious threat in terms of cyber terrorism at the moment, but should a group acquire the necessary technical capabilities they could hack strategic systems if IoT technologies with access to critical information or control of infrastructure.

Furthermore, it should not be ignored that while terrorists might not be there yet, governments are actually developing deadly cyber capabilities. The United States has outsourced a $460 million project to private companies to develop cyber weapons that could target human lives. These reportedly might consist in provoking a nuclear meltdown, opening a dam with the intent to harm individuals and undermining air control systems to induce a plane crash (Sternstein, 2015). While the US military is developing the project in accordance with international law, this sets a precedent that risks inspiring terrorists, giving them actual existing weapons to be studied and replicated.

The analysis presented in this section reveals how in the future threat landscape there is the potential for deadly attacks carried out simply through the use of a computer. This fits the conclusion of the theoretical part of this paper, which argued that while at present terrorists are using the Internet to coordinate attacks, in the future they might use it to execute the attack itself. The good news is that governments seem to have a head start on the matter and probably have the time to develop appropriate counter measures (Sternstein, 2015). The bad news could be the beginning of a new generation of deadly cyber weapons that might eventually fall in the hands of terrorists too. It is hard to determine how and when this could happen, yet it is a scenario that should not be ruled out, especially in light of the tenacity of groups such as IS or the Taliban.

Discussions and conclusions

The first part of this paper sought to define cyber terrorism, drawing from different international sources. These ranged from institutional ones, to law enforcement and academia. The analysis delved into several interpretations of it, with two main views emerging:

a) The idea of cyber terrorism involving the computer as the main or only weapon
b) The concept of the machine as a tool to sustain a terrorist group (with financial resources and manpower) and plan attacks.

The second and third parts then focused on comparing theory with facts, to show which of the two main schools of thought was the most appropriate. Taking as examples the Taliban and IS, two highly cyber active terrorist groups, the second section revealed that at present terrorists are mainly using the Internet in coordination with physical actions. Differently, the third and final part of the paper highlighted how in the future there is a scenario where cyber terrorists might develop the necessary knowledge to strike a deadly cyber attack using a computer as the only weapon. This concept is strengthened by the fact that governments are already trying to build such weapons and that the evolution of technology (especially with the Internet of Things), is presenting new opportunities as well as challenges in terms of cyber security.

Another major takeaway from this paper is for businesses. Any business could be the victim of social engineering or phishing emails aimed at funding terrorist groups; hence, there should be the adequate level of awareness among employees. In addition, companies could be a symbolic and highly valuable target of attacks, and they should adopt adequate security measures. This paper has shown how cyber attacks and terrorism are great reasons for concern for both the public and the private sector; therefore it would be unwise to underestimate the two of them combined. This is especially (but by no means exclusively) important for those dealing with critical assets, such as infrastructure, power plants, public transport.

This paper also recommended accuracy when using the word cyber terrorism, in order to distinguish it from cyber crime. The first part of the paper, focusing on definitions, aims exactly at shedding some light on a term that is sometimes used inappropriately due to a lack of agreement on its meaning. Indeed, understanding the shape and size of the problem is the very first step to solve it, and it is a step that has not been made yet.

Research limitations and direction for further research

Further research may be suggested to explore new technologies and their links to terrorist groups, to dig into their technical skills and how likely it is they might represent a serious threat in the future, and whether this would be in the short, medium or long term. This paper is not written from a highly technical point of view, hence threats represented by new technologies such as IoT are not dealt with in their specifics. With this premise, the third section of this paper should be also seen as a suggestion for experts to delve more deeply into the matter.

Bibliography

Alcantara, P. and Riglietti, G. (2016). *Horizon Scan Report 2016*. Horizon Scan report. [online] Reading: The Business Continuity Institute, p.11. Available at: https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_HackingForISIS_April2016.pdf [Accessed 28 Jul. 2016].

Alkhouri, L., Kassirer, A. and Nixon, A. (2016). *Hacking for ISIS: The Emergent Cyber Threat Landscape*. [online] Flashpoint, pp.2-25. Available at: https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_HackingForISIS_April2016.pdf [Accessed 28 Jul. 2016].

Awan, I. (2014). Debating the term cyber terrorism: issues and problems. *Internet Journal of Criminology*, [online] pp.1-10. Available at: http://www.Internetjournalofcriminology.com/awan_debating_the_term_cyber-terrorism_ijc_jan_2014.pdf [Accessed 28 Jul. 2016].

Baranetsky, V. (2009). *What is cyberterrorism? Even experts can't agree*. [online] Harvard Law Record (through the Internet Archive). Available at: https://web.archive.org/web/20091112093639/http://www.hlrecord.org/news/what-is-cyberterrorism-even-experts-can-t-agree-1.861186 [Accessed 28 Jul. 2016].

Bodkin, H. (2016). Terrorist groups acquiring the cyber capability to bring major cities to a standstill, warns GCHQ chief. *The Telegraph*. [online] Available at: http://www.telegraph.co.uk/news/2016/06/08/terrorist-groups-acquiring-the-cyber-capability-to-bring-major-c/ [Accessed 28 Jul. 2016].

Denning, D. (1999). Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy. In: *The Internet and International Systems: Information Technology and American Foreign Policy Decision Making*. [online] San Francisco: The World Affairs Council, pp.239-288. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf [Accessed 28 Jul. 2016].

Gordon, S. and Ford, R. (2003). *Cyberterrorism?*. [online] Symantec, pp.3-10. Available at: https://www.symantec.com/avcenter/reference/cyberterrorism.pdf [Accessed 28 Jul. 2016].

Gwakh, B. (2011). The Taliban's Internet Strategy. *Radio Free Europe Radio Liberty*. [online] Available at: http://www.rferl.org/content/the_talibans_Internet_strategy/24323901.html [Accessed 28 Jul. 2016].

Hairan, A. (2011). A Profile of the Taliban's Propaganda Tactics. *The Huffington Post*. [online] Available at: http://www.huffingtonpost.com/abdulhadi-hairan/a-profile-of-the-talibans_b_442857.html [Accessed 28 Jul. 2016].

Hern, A. (2016). Taliban app removed from Google Play Store. *The Guardian*. [online] Available at: https://www.theguardian.com/technology/2016/apr/04/taliban-app-removed-from-google-play-store [Accessed 28 Jul. 2016].

InfoSec, (2012). *Cyberterrorism Defined (as distinct from "Cybercrime") - InfoSec Resources*. [online] InfoSec Resources. Available at: http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/ [Accessed 28 Jul. 2016].

Institute for economics & peace, (2015). *Global Terrorism Index 2015*. Global terrorism Index. [online] Institute for economics & peace, pp.20-24. Available at:

http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf [Accessed 28 Jul. 2016].

Krasavin, S. (2016). *What is Cyber-terrorism?*. [online] Crime-research.org. Available at: http://www.crime-research.org/library/Cyber-terrorism.htm [Accessed 28 Jul. 2016].

Lewis, J. (2016). *Managing Risk for the Internet of Things*. [online] Center for Strategic & International Studies, pp.9-12. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160217_Lewis_ManagingRiskIoT_Web_Redated.pdf [Accessed 28 Jul. 2016].

Majoran, A. (2014). Terrorism & the Oxygen of Publicity - Mackenzie Institute. [online] Mackenzie Institute. Available at: http://mackenzieinstitute.com/terrorism-oxygen-publicity/ [Accessed 13 Oct. 2016].

O'Brien, D. (2014). *The Internet of Things: New Threats Emerge in a Connected World*. [online] Symantec Security Response. Available at: http://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world [Accessed 28 Jul. 2016].

Statista, (2016). *IoT: number of connected devices worldwide 2012-2020*. [online] Statista. Available at: http://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ [Accessed 28 Jul. 2016].

Statista, (2016). *Terrorist attacks in 2015, by country*. [online] Statista. Available at: http://www.statista.com/statistics/236983/terrorist-attacks-by-country/ [Accessed 28 Jul. 2016].

Sternstein, A. (2015). *Pentagon Contractors Developing Lethal Cyber Weapons*. [online] Nextgov. Available at: http://www.nextgov.com/cybersecurity/2015/11/lethal-virtual-weapons-real/123417/ [Accessed 28 Jul. 2016].

Tafoya, W. (2011). *Cyber Terror*. [online] FBI. Available at: https://leb.fbi.gov/2011/november/cyber-terror [Accessed 28 Jul. 2016].

The Economist Data Team, (2015). The plague of global terrorism. *The Economist*. [online] Available at: http://www.economist.com/blogs/graphicdetail/2015/11/daily-chart-12 [Accessed 28 Jul. 2016].

United Nations Office on Drugs and Crime, (2012). *The use of the internet for terrorist purposes.* [online] United Nations Office on Drugs and Crime, pp.3-13. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [Accessed 28 Jul. 2016].

Williams, T. (2016). The Cyber Threat and Terrorism. [online] Contextis.com. Available at: https://www.contextis.com/resources/blog/cyber-threat-and-terrorism/ [Accessed 13 Oct. 2016].