The Study of the Plight of Cyberterrorism and Its Way Out

Mingyang Gao[1], Yingjie Dong[2], Xueding Qiao[3], Shuo Fan[4]

[1]School of International Relations, Xi'an International Studies University, Xi'an 710000, China
[2]Shenzhen Academy of International Education, Shenzhen 518000, China
[3]Qingdao No.2 Middle School of Shandong Province, Qingdao 266001, China
[4]Rabun Gap Nacoochee School, Rabun Gap 30568, United States

Abstract: *After "9.11", terrorist attacks have been increasingly relying on cyberspace, posing an imminent threat to national security. This article introduces two types of cyberterrorism attack: target oriented and tool oriented. Target oriented attack means terrorists directly attack networking device, while tool oriented is the activity making use of Internet tools. Moreover, in the work, three countermeasures and five futures for cyberterrorism are also discussed. This article suggests that understanding cyberterrorism in a board sense, and do not underestimate the serious situation.*

Keywords: *Cyberterrorism, Target oriented, Tool oriented, National security, Countermeasures*

1. Introduction

There is not a universally definition for terrorism or its new form—cyber terrorism. People would sometimes disagree about whether the definition fits particular incidents. The word 'terror' which originated from Latin means 'to frighten' and to 'intimidate'. A general definition for cyber terrorism could be "It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. As cyberterrorism has been considered with more and more seriousness from both the public and the government, whether it is target oriented or tool oriented, cyberterrorism is a serious threat to national security in present and future.

In section one, the target oriented cyberterrorism background and the reasoning behind cyberattacks will be discussed. It will present how the development of cyber-technologies and cyber-attacks are closely bonded. Since there is a lot of potential prey for cyber attacks, we have categorized them into four most important categories, individuals, governments & infrastructures, military forces, firms & corporations, each of these would be examined and analyzed closely. In section two, the tool oriented which is the counterpart of section one would be presented. Topics like 9/11, and its connection to the spread of cyber-attacks would be shown. In section three, cyberterrorism as a whole would be summarized and explained. The potential scenarios of previously discussed topics, in sections one through three would be presented and explained.

2. Target Oriented Cyberterrorism

The innovation of technologies enables terrorists to exploit the internet and to achieve malicious actions. Many reasons triggered cyber-attackers, such as terrorists, to launch cyber-attacks. Those reasons can be concluded to three factors, disagree with the government, disagree with certain socio-cultural groups, and for economic purposes. All of those three reasons mentioned above became the reasons to trigger cyber-attackers, such as terrorists, to launch cyber-attacks[1].

The definition of target-oriented attacks is for terrorists to launch attacks using the internet. This section of the paper will present the approaches that terrorists can adopt to launch cyber-attacks and the victims under cyber-attacks. The victims under cyber-terrorism-attacks are individuals, governments, infrastructures, military forces, and corporations.

2.1 Individuals

Individuals, such as citizens, are one of the targets under cyberattacks launched by terrorists. There are two main types of attacks that terrorists can launch against individuals, which are information theft and Denial of Service attack. Cyber information theft is the malicious action taken by terrorists to stole the critical information from individuals. Citizens store their personal information into cyberspace, which provides opportunities for malicious attackers such as terrorists to abuse cyberspace and attack the victims—every piece of information, such as identity, data, bank accounts, locations, and even pictures — have the potential to get by cyber attackers such as terrorists[2]. Not only we have personal information stolen from terrorists, we also have the denial of service attack launched by terrorists. Denial of Service attack can be employed to disable users' access to the internet or simply to cut off the connection between users and their connected facilities(5G). The problem of denial service is going to continue its existence in the 5G era[3]. Methods used by terrorists to attack individuals are also applicable to governments and infrastructures. However, there are more approaches that terrorists could take to launch cyber-attacks on governments and national infrastructures.

2.2 Government and Infrastructures

Governments and infrastructures are also the targets under cyberattacks that have been launched by terrorists. The purpose of launching those cyber-attacks was mainly for information acquisition, order disruption, and service malfunction. The types of attacks were varied when it comes to attacking governments and infrastructures. Some attacks directly focus on the government, and some attacks focus on government controlled national infrastructures.

Some attacks have launched to attack governments by terrorists were mainly to steal government information. The governments store their essential information and data on the internet, and terrorists can attack their internet to obtain sensitive information and data[1].

Aside from directly attack the government, terrorists can adopt more ways to attack critical national infrastructures. Many different kinds of cyber terrorism attacks focus on government and national infrastructures, such as shutting down services, controlling critical infrastructure systems, cutting off communications, creating flooding, spreading false information, and other attacks. In 2001 the US root servers received a denial of service attack that shut down their servers for 6 hours. In the same year in 2001, one of Australia’s sewage systems has been under attack, which the attacker gains control of the sewage management system and release a large amount of sewage into public parks. In 1997, a cyber attacker attacked one of the Federal Aviation Administration control towers, which have disabled the communications of the airport. Also, in 1998, the Sri Lankan government’s official website has received a high flooding attack launched by terrorists. Those attacks mentioned above cause disruption, malfunction, and destruction to a nation[4].

2.3 Military Forces

There are different forms of attacks that terrorists can use to attack military forces, such as Denial of Service, Espionage, viruses, and other forms that targeted the infrastructures, operations, functions, systems, and services inside military forces. The internet has become a useful tool for terrorists to launch attacks. In the past 20 years, military forces were under attack by terrorists. Attacks were launched by terrorists to disable normal functions of military facilities in the United States, Iran, and other nations. Such as in 2008, 2010, and 2011 different military forces in the United States were under attack by terrorists[4].

2.4 Firms and Corporations

Businesses and corporations can be attacked by terrorists through espionage activities[4]. Businesses store their essential data and information online, and that information is not well protected enough. Information and data loss can lead to a business losing money. Also, sometimes those cyber-attacks launched beyond the national borders, which make those espionage activities hard to trace, to prevent, and to resolve[5].

Overall, the targets under target orient attacks are individuals, governments, infrastructures, military forces and corporations. This type of attack mainly focusses on espionage, disruption, and malfunction of those targets’ internets or target themselves.

3. Tool-oriented Cyberterrorism

A broad approach to cyberterrorism definition involves traditional terrorists using internet as a means for preparing and launching attacks, but not directly causes damages to individuals and infrastructures.

After “9.11", governments worldwide called for stronger actions against terrorism. Since the living space for traditional terrorists was squeezed, they turned to the cyberspace to survive. Meanwhile, the widespread availability of internet largely facilitates their activity: It is inexpensive and relatively easy to operate, having lower threshold than traditional military attack; using anonymous or assumed false identities makes it hard to identify the attacker; besides, internet is so influential that messages and instructions can easily cross geographical boundaries. Those advantages make internet a preferred tool for terrorism activities.

There are five types of activity that terrorists using internet tools to carry out.

3.1 Propaganda

Terrorists are giving increasing attention to online propaganda. Ayman al-Zawahiri, current head of al-Qaeda once said, “We [al-Qaeda] are in a battle, and more than half of this battle is taking place in the battlefield of the media[6]. Al-Qaeda, ISIS and other terrorism groups have built specialized media centers and publicity teams. Terrorist propaganda strategy mainly has two features. Firstly, widely distributed audiences. Their propaganda is not only aimed at Muslim groups, but also mobilizes foreign extremists to fight against their governments. Secondly, professional productions with high quality. Specialized teams in terrorism groups work on streamlining videos and magazines, and translate them into different languages before sending to the audience. A highly publicized instance was a slickly produced video of the beheading of American journalist James Foley in August 2014[7]. Thirdly, highly inflammatory. Charlie Winter classified five kinds of terrorist narratives: mercy, victimhood, war or military gains, belonging and utopianism[8]. Facts proved that well-designed narrative has made great effect in radicalizing: In October 2014, three teenage girls from Denver were heading to Syria to join Islamic extremists after browsing their websites[9]. And similarly stories are repeated frequently in the news.

3.2 Recruitment

Online chatting rooms and apps has replaced mosque becoming the recruitment center for terrorists nowadays. Internet connects people around the world to form virtual communities and enables real time interaction. There are two features of terrorist recruitment strategy. Primarily, they value young and professional technician in recruitment. Young technician can adapt to the fast-changing online environment well and improve the quality of propaganda productions distributed on social medias. Besides, they pay attention to recruit foreign fighters. “Lone wolf” attackers are more likely to conduct a successful attack for being in the heart of a foreign state. As a result, the number of “lone wolf” attacker has been growing. Government estimates on the number of Americans joining IS have varied around the range of approximately 30 to 100. Estimates for UK are similarly difficult but usually higher—news reports have cited 500 British citizens affiliated with IS in Syria and Iraq[7].

3.3 Fund raising

Sufficient funding is the blood of any terrorism activity. Terrorists raise funds with the help of internet from two aspects. One is directly seeking donation from social media, releasing statements on apps like Facebook, Twitter and Skype, asking supporters and sympathizers around the world to donate. Another way is conducting crime in cyberspace, including breaking into the system to steal credit card passwords, identity theft and online gambling.

3.4 Training

The development of Internet greatly reduced the gap in receiving education and training. Extremists can accept terrorism training remotely, learning advanced and effective techniques of terror attack online. Their courses includes attack strategy, instructions for making and using guns, ammunition, poisons and explosives. For instance, the perpetrator of Boston Marathon bombing in 2013 confessed that he learned the technique of bomb-making from Al-Qaeda’s online publication *Inspire.*

3.5 Communication

Due to the convenient online communication, organizational structure of terrorists has been increasingly scattered. Internet facilitates independent terrorism action and therefore, produces loose and headless terrorism organizations. Terrorists can communicate, coordinate, control and command worldwide using internet, instead of gathering together at a real place, which reduces the likelihood of being caught. Each terrorist is like a node connected by online tools to form a network, and the destroy of any node would not largely affect the whole terrorism network.

4. Threat Assessment of Cyberterrorism

In recent years, with the rapid growth of cyberterrorism, cyberterrorism has gradually begun to threaten all aspects of various countries. Terrorist activities conducted on the Internet have become worse and worse. For the victims, the consequences of these activities may be devastating and irreversible.

4.1 National security

By locking and polluting computers, cyber terrorists restrict or even worsen the diplomatic relations between countries or regions, causing virtual interruption. They also gain the control of traffic networks such as nuclear weapon activation codes, missile launcher parameters and so on by hacking into government networks. Thereby threatening the security of citizens of all countries.

4.2 Financial risks

Due to the globalization of trade, the economy of one country, especially developed countries, has been hit by cyber terrorism, and then the economy of the whole world will be hit hard, leading to the economic breakdowns, temporary failures in providing products and services, aggravating conflicts between classes and classes, countries and countries, and even coups. The 1929-1933 economic crisis in the United States fully demonstrated the world as a whole and its serious consequences.

4.3 Social risks

Cyber terrorists steal users' personal information, fabricate facts and upload them to social media in order to damage or distort the reputation of victims and lead the government loses the trust of citizens due to the loss of their personal privacy data.

4.4 Infrastructural risks

When cyber-terrorists break into countries' infrastructure management systems through the Internet, they will pass through the pollution of the environment, such as the discharge of industrial wastes into dams, traffic accidents, such as a collision between two planes or trains, resource paralysis, like resulting in massive power outages to poses a threat to the lives of citizens, causes panic among citizens, makes citizens dissatisfied with the government, and causes social unrest.

In order to combat cyber terrorism, governments often seek international cooperation or social help, but various problems, including financing, make it necessary for governments to face various new challenges in solving these problems.

4.5 Different understandings of risks, responsibilities and techniques

Each country has a different understanding of the level of danger, its own responsibilities, and the extent to which it shares technology. There will always be countries that condemn the response of another country, which leads to differences and complaints among countries, leading to the loss of the possibility of cooperation between countries.

4.6 Reluctance of governments to share data and information with potential rivals

Like the confrontation between Russia and the United States over ISIS, countries do not disclose their intelligence for free for the sake of their own interests, and even the issue of intelligence sharing has strained relations between the two countries in the past

4.7 The costs of cybersecurity protocols and infrastructure, and ‘free riding’

The government needs a large amount of funds to fight against cyber terrorism, and many developed countries are unwilling to use their own funds to fight against cyber terrorism due to interest factors. As a result, many countries that invest in this field start to stop investing in this field because they think their own interests are violated. The government seeks investment from all sectors of society. Meanwhile, the investment demand of the government will make all sectors of society panic about terrorism and lead to the decline of citizens' trust in the government. The costs of investment in cybersecurity protocols and infrastructure always come with the risk of ‘free-riding’[10]. Countries want others to take responsibility and enjoy their own convenience, so there will be no government finally take concrete measures to deal with cyber terrorism.

5. Conclusion

This article has sketched two sides of cyberterrorism attack and laid out risks and challenges that they posed to national security. As noted above, terrorists are increasingly relying on internet to prepare and conduct attack, causing damages to infrastructure and personal safety. However, there are contrasting views on the level of threat the situation poses, with some believing that cyberterrorism is a serious threat at present and others arguing that the threat has been exaggerated because we haven’t seen any casualties in cyberterrorism attacks so far. In this article, we suggest understanding cyberterrorism in a board sense, and do not underestimate the serious situation. Terrorists already have the capacity to launch cyber attacks at present, since requiring information technology are growingly easier, terrorism will become more formidable and intractable in the future, especially if they break into the control system of nuclear weapon. Therefore, it is necessary for governments to figure out responses that may mitigate the crisis.

5.1 The Three Countermeasures for Cyberterrorism

Three possible countermeasures are suggested in this article:

Firstly, technical means is the key measure. The battle between cyberterrorists and governments is essentially a contest of network technology. Governments can take actions like updating firewall, using access lists to protect network facilities of critical infrastructure in military, energy, electricity, transportation and other areas.

Secondly, laying more emphasis on globalized law enforcement. Governments should make sure that domestic laws aligned with international laws, so that would not cause differences and difficulties to judicial practice. Besides, it is important to strike a balance between adopting real-name system and protecting private rights. For example, allowing anonymity at the front-end and verifying user’s real identity at the back-end.

Thirdly, creating intelligence pool and sharing platform to enhance international cooperation. The effective solution of cyberterrorism needs the joint efforts of all countries. Establishing unified standards and coordinating organizations will help reduce the phenomenon of “free-riding” and unnecessary rivalry between states.

5.2 The five futures for cyberspace and cyberterrorism

The future of cyber space is going to be discussed in the latter paragraphs. There are five possible futures for the cyber space which is Status Quos, Conflict Domain, Balkanization, Paradise, and Cybergeddon. Those five possible futures for the cyber-space will lead to 5 possible changes that will occur on cyber-terrorism itself.

The first future is known as Status Quo. This future indicates that the cyberspace will remain its current condition. There is no apparent disastrous attack, and yet there are anticipations from people to expect a massive attack. There is a kind of “underlying stability” in cyberspace. Cyber-terrorism will be very similar to what this paper is discussing[11].

The second future is known as Conflict Domain. Th future for cyberspace as a conflict domain will make the cyberspace divided into different domains. There are certain domains in the cyberspace that is safe for regular life activity, but there are also domains which frequently enables malicious activities. Nations are going to attack each other’s cyberspace in particular cyber domains, and there will be cyber domains that enable frequent terrorists’ activities online[11]. The third future is known as balkanization.

Nations run their internet, and the internet will not be as open as it was now. Nations can deny foreign users' access to their internet. Cyber terrorism from this perspective will not thrive because balkanization internet can enhance the level of cybersecurity for nations. Therefore, it is reasonable to have the anticipation that cyber terrorism will not be a severe threat in a balkanization internet[11].

The fourth future is known as Paradise. The future for cyberspace in the form of paradise future is exceptionally safe. There are new technologies that guaranteed the security for the cyberspace. Nearly all attacks can be smothered in the paradise future, which means that cyber-terrorism is going to survive and thrive in the Paradise future[11].

The fifth future is known as Cybergeddon. In the Cybergeddon future, defensive technologies are useless. It is impossible to prevent any attacks, and the whole cyberspace is exceptionally unsafe. Cyber-terrorism can thrive in the Cybergeddon because of its natural geography, which offense is stronger than defense[11].

Finally, it is worth reiterating that cyberterrorism is a serious threat to national security both in present and future. We realize that our analysis is only a brief outline and we also understand that not all counterterrorism policies can be predicated and adopted to effectively eliminate attacks. What becomes clear in this brief essay is that we should be vigilant in peace time and that forethought prevents calamity.

References

[1] Robin A Gandhi, William Sousan, Phillip A. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," IEEE Technology and Society Magazine, Vol. 30, No. 1 (2011), pp. 28-38

[2] For more information about cyber information theft, please visit L. D. Roberts, D. Indermaur, C. Spiranovic, "Fear of Cyber-Identity Theft and Related Fraudulent Activity," Psychiatry, Psychology and Law, Vol.20, No.3(2013), pp.315-328

[3] For more information about denial service attack, please visit Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov," Overview of 5G Security Challenges and Solutions," IEEE Communications Standards Magazine, Vol. 2, No. 1 (2018), pp. 36-43

[4] A. Al. Mazari, A. H. Anjariny, S. A. Habib, E. Nyakwende, "Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies," International Journal of Cyber Warfare and Terrorism, Vol.6 (2016), pp. 1-12

[5] Gerald O'Hara, "Cyber-Espionage: A growing threat to the American economy," CommLaw Conspectus, Vol. 19 (2010), pp. 241-275.

[6] Joseph Lieberman and Susan Collins, Violent Islamist extremism, the internet, and the homegrown terrorist threat (Washington D. C.: United States Senate Committee on Homeland Security and Governmental Affairs, 2008)

[7] Anne Aly, Stuart Macdonald, Lee Jarvis & Thomas M. Chen, "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization", Studies in Conflict & Terrorism, Vol.40, 2017

[8] Charlie Winter, The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy (London: The Quilliam Foundation, 2015).

[9] Ben Brumfield, "Officials: 3 Denver girls played hooky from school and tried to join ISIS", CNN, October 22, 2014, accessed August 30, 2015, http://edition.cnn.com/2014/10/22/us/colorado-teens-syria-odyssey/index.html.

[10] Lee Jarvis, Stuart Macdonald, "Responding to Cyberterrorism: Options and Avenues", Georgetown Journal of International Affairs (Fall 2015), pp.134-143.

[11] Atlantic Council, "The Five Futures of Cyber Conflict and Cooperation," https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-five-futures-of-cyber-conflict-and-cooperation/ (Accessed: 07-02-2020).