Zuberi *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003(Online)

LGU International Journal for
Electronic Crime Investigation

Research Article Vol. 2 issue 1 January-March 2018

Use of Cyber Space by Terrorist Organizations

Kaukab Jamal Zuberi
Digital Forensic Research and Service Centre
Lahore Garrison University

Abstract:

Prevention of Electronic Crime Act 2016 of Pakistan, defines and include cyber terrorism as a cyber-crime. Due to its anonymity cyber space is a popular tool used by terrorists. Terrorists use cyber space to launch their propaganda, recruit new workforce, radicalize target groups, raise financing, train the new recruits or upgrade the skills of existing workforce, raise funding for their operations, establish communication infrastructure to communicate within and outside the organization and execute their operations. This article discusses the various ways cyber space is used by the terrorist organizations to execute their plans.

Keyword: Terrorism, Cyber terrorism, Propaganda, Terrorist financing, Terrorist recruitment, Terrorist training, Radicalization, Direct Soliciting

1. Introduction

Prevention of Electronic Crime Act 2016 (PECA) was passed on August 11, 2016 in Pakistan. In this act, 25 new offences and their punishments were introduced. Section 10 of PECA deals with cyber terrorism. According to PECA whoever commits or threaten to commit any of the following offence:

a) Coerce, intimidate, create a sense of fear, panic or insecurity in the government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society.

b) advance interfaith, sectarian or ethnic hatred

c) advance the objectives of organizations or individuals or groups proscribed under the law

Section 10(a) mentions that it is punishable offence to prepare or disseminate information through any information system or device that advances inter-faith, sectarian or racial hatred.

Section 10(b) mentions that recruitment, funding and planning of terrorism, preparing or disseminating information, through any information system or device, that invites or motivates to fund, or recruits people

for terrorism or plans for terrorism, is a punishable offence. Punishments under Section 10, 10a and 10b are mentioned in the Act.[1]

PECA has established cyber terrorism as a criminal offence in Pakistan punishable by law.

Terrorists cannot live on idealism alone. They have to propagate their ideology, gain support, hire recruits, raise funding in order to carry out their plans effectively. Internet is one of the easiest and effective way of propagating, hiring, fund raising and often to carry out the plans. In this article, we shall discuss the means and ways to hire new recruits through internet.

2. Propaganda

Merriam-Webster defines propaganda as “ideas, facts, or allegations spread deliberately to further one's cause or to damage an opposing cause;” [2]

Terrorist organizations use emails, messaging applications, presentations, multimedia files, cartoons, animations and video games developed by themselves or their supporters too propagate their cause. Such tools are then distributed through internet using dedicated websites, chat rooms, secret forums, online magazines, social networking websites, and popular file-sharing websites. Recent video based social media apps are also a popular tool for such propaganda as private video chat rooms can be created on several of these websites. The use of indexing services such as Internet search engines also makes it easier to identify and retrieve terrorism-related content.

Dark web is a popular medium of propagating and distribution of the of these organizations.

There are multiple objectives and large range of audience for the propaganda done by terrorist organizations. The propaganda is targeted at potential or existing supporters. It is focused on recruitment, radicalization and incitement of terrorism through messages which glorify the accomplishment, dedication and achievements of extremist goals.

2.1 Recruitment

Terrorist organizations use password protected websites and internet chat groups for clandestine recruitment. Effective propaganda tools are used to lure marginalized and vulnerable groups in the society. The process of recruitment capitalizes on the sentiments of the targeted groups. It focuses on the sentiments of injustice, exclusion or humiliation. Internet can be used as an effective medium to hire not only young professionals, students and minors which comprise the high ratio of internet users. They lure them through cartoon, internet games and children stories with messages promoting and glorifying the acts of terror, such as suicide attacks

2.2 Incitement

Material prepared to incite an act of terrorism is different from the material prepared to propagate a cause. For example, the dissemination of material on instructive material on the use of explosive would not be considered a breach of law unless the material incites the readers to commit a terrorist act or the material could be used for a terrorism purposes.

Communication through internet can

be very manipulative and dangerous if it is used by trained recruiters of terrorist organizations. They successfully influence the young minds by using latest communication techniques. They use chat room, video chats, private video chats, and other social media websites to incite young victims.

2.3 Radicalization

Radicalization refers primarily to the process of indoctrination that often accompanies the transformation of recruits into individuals determined to act with violence based on extremist ideologies. Radicalization does not belong to one group or one religion. There are some common root causes for radicalization. They are communal reasons and personal reasons. However, we cannot generalize them. Communal reasons are mentioned as follows:

1. Large minority population which is politically, socially and economically marginalized.
2. Certain communities to be treated as "suspect groups". Treatment is invasive and overbearing counter terrorism efforts.
3. Cultural or Political hostility against a religion.
4. Unpopular foreign policies, such as support for repressive regimes or involvement in a military campaign.
5. The presence of preexisting recruitment networks

The examples of personal reasons are as follows:

1. Personal ties with radicalized person.
2. A desire for adventure, rebellion, and life experience.
3. Need to belong to a group
4. Feelings of compassion and concern for the suffering of others with whom one feels some kind of personal connection, such as one's co-religionists.
5. Presence of teen angst.

Internet, Prisons and ties with radicalized friends remain some of the most common causes of radicalization. In the end, external factors are more influential in the process of radicalization.

Recruitment, Incitement and radicalization can be viewed as point along with a continuum to terrorism. [3]

3. Financing the Terrorist Operations

A terrorist organization requires resources to survive and conduct its operations. Detailed budget or requirements are seldom listed in terrorist operations and they vary from one operation to another, we can generalize the minimum categories of minimum requirements for such operations. These resources can be divided into three categories:

a) Money and other negotiable instruments.

b) Tangible resources – those goods that have monetary value.

c) Intangible resources – those resources which do not have monetary value. Some of intangible resources are traded for money. For example, a terrorist organization training another organization for money.

The resources also vary as some organizations take care of families of those who die in their operations and other provide handsome salaries and benefits to their recruits. Therefore, the resources vary from organization to organization and operation to operation. A terrorist organization needs nancial resources for the following:

- Recruiting new members
- Establishing and maintaining training camps and bases
- Maintain the housing requirements and day to day needs.
- Buy equipment, explosives, conventional and unconventional weapons
- Buy or create forged identity and travel documents.
- Acquire technologies for intelligence gathering.
- Create a communication network
- Bribe government officials and other sources as and when required.
- Day-to-day maintenance expenses for members awaiting commands to launch Operations [4]

Terrorists use various means to raise funding for their operations. Cyber space due to its anonymity and large access is a popular medium to collect funds. Some of the methods used to raise funding include:

- Direct Soliciting
- E-Commerce websites
- Exploitation of online payment tools
- Charitable Organizations

3.1 Direct Soliciting

Direct Solicitation include contacting the potential financers through use of websites, mass mailing, chat rooms and targeted communications [5]

3.2 E-Commerce Websites

E-Commerce websites may sell books, videos, training material or other items to collect money through credit cards and other online payment services like paypal etc. The introduction of crypto currencies has enabled the terrorists to conceal their identity and accept payments from anonymous resources.

Terrorist may also use dark web to sell illegitimate goods and services and raise funds through such websites.[6]

3.3 Exploitation of online payment tools

Terrorists use various hacking techniques to steal identity information (social security numbers, etc.), credit card numbers, wire fraud, auction fraud, hacking mining machines and crypto currency exchanges and online payment facilities like PayPal.[7]

3.4 Charitable organizations

Terrorist create fake charitable organizations and raise money on those organizations. These web based organizations are seemingly legitimate. Some terrorist group create shell companies to raise charities for philanthropic purposes. These companies use names to emotionally exploit the sentiments of the donors. Most of the donors are unaware of the motives behind collection of these funds and they donate their charities in good faith. Social media is also used as a fund raising tools

by terrorist organizations. Terrorist receive payments from supports and unsuspecting donors, who believe that they are donating for a humanitarian cause. [8]

4. Training

Due to the ease of access, internet has become a popular medium to distribute training material. This training material vary from videos uploaded on YouTube to pdf documents on compromised websites.

Internet has become a virtual training ground for these organizations. Such websites and social media is used to spread training materials and training videos. Websites suddenly emerge and disappear after serving the purpose. Insufficient information security structures have made websites vulnerable and once these websites are compromised anonymous web pages can be uploaded known to a specific group of individuals.

Ease of access, lack or insufficiently qualified monitoring force, lack of qualified cyber security personnel at public or private organizations have contributed towards the misuse of cyber space for training purpose.

Instructional material on such websites includes tools for counter intelligence and hacking. Terrorists are trained with these technologies to facilitate their anonymity and online communication. [9]

5. Planning

Various internet technologies are used in communicating within and between organizations. The communication is extremely sensitive at this stage and carry the promotion of extreme violence. Plans are discussed within the organization, with other organizations present in the country and across the border. Instructions are shared with maps, directions, photographs, technical details like how to use explosives and other tools to execute a plan. Often these instructions are hidden in graphic or multimedia files using steganography tools. Modern steganography tools are easily available on web. These tools are not expensive and can successfully hide information in graphic and multimedia files which is very difficult to detect. Sometimes, the communication is done through public networks, internet cafes and other social media services and is encoded. Whereas, sometimes the communications is done through proprietary communication tools developed by the organizations.[10]

6. Execution

Execution is the actual attack to disrupt critical infrastructure of a country or a critically important organization and spread terror among the citizen of the country. The attack may be a physical attack or a cyber-attack. In both cases, internet is used to communicate securely to make the attack successful. A cyber-attack is the exploitation of computer network and manipulation of data to disrupt the operations. These attacks are made through hacking, advanced persistent threats, viruses, malwares or other malicious means of access to the network.Terrorists organizations may decide not to disrupt the network once it is compromised. They may decide to steal the sensitive data and use it to their advantage. There is a secondary market on dark web which is always ready to buy such data. Moreover, the terrorist organization may decide to use the stolen data for their own advantage. Such data includes diagrams, drawings, phone numbers and family details of senior military officers etc. [11]

7. Conclusion

Terrorists use internet to recruit, train, plan and execute their operations. Internet is also used in raising finance to fund their operations. In this process they keep their anonymity and utilize secure communications tools available on the social media and in cyber space.

There is a need to develop sophisticated tools to prevent, detect and deter cyber-attacks. Surveillance teams with multi-linguistic knowledge should be created and they should monitor the chat rooms and other social media websites. Cooperation should be developed with similar agencies in different countries.

Pakistan being in the middle of terrorist activity have suffered in last few decades of war in Afghanistan. More than 80,000 Pakistanis have been killed in the war of terror since 2003. Incidents of Cyber terrorism are not reported openly in Pakistan. We need to create teams with private sector contribution to develop preventive mechanism against cyber-attacks.

8. Reference

[1] NATlONAL ASSEMBLY SECRETARIAT. (2016). “Prevention of Electronic Crime Act” May 2016. Islamabad. Available at: http://www.na.gov.pk/uploads/documents/1472635250_246.pdf.

[2] Merriam-Webster https://www.merriam-webster.com/dictionary/propaganda.

[3] Simon Shercliff Sue Hemming OBE The Use of The Internet For Terrorist Purposes page no 6 (2012) United Nations, UNODC.

[4] Jodi Vittori. “Terrorist Financing and Resourcing” page 19-23, Palgrave Macmillan 2011.

[5] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7 (2012) United Nations, UNODC.

[6] Babak Akhgar Andrew Staniforth Francesca Bosco- Cyber crime and cyber terrorism investigator's handbook-Syngress, , Elsevier Inc. Page 153 (2014).

[7] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7 (2012) United Nations, UNODC.

[8] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7 (2012) United Nations, UNODC.

[9] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 8 (2012) United Nations, UNODC.

[10] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 8-11 (2012) United Nations, UNODC.

[11] Simon Shercliff Sue, Hemming OBE. “The Use of The Internet For Terrorist Purposes” page no 7-10 (2012) United Nations, UNODC.