CYBER TERRORISM: A CASE STUDY OF ISLAMIC STATE

Zaheema Iqbal*
Khurram Iqbal**

Abstract

In today's postmodern world with the latest and top notch internet technologies in the market, if it has become easy and accessible for everyone to communicate with others sitting at the other corner of the world, it has also given rise to the cybercrimes including cyber terrorism which has not only provided grave threats to the whole world but also posed a question of whether with the manipulation of cyber space, cyber terrorists can damage or destroy the physical infrastructure of its target. Owing to easy access to everyone and strong damage done as compared to traditional terrorism, today terrorists are relying on cyber terrorism as well. The Islamic State (IS) has emerged as one of the brutal and violent terrorist organizations which hired cyber experts and manipulated cyber space to the extent that today they are most active and professional cyber users' terrorist organization of the world. The main focus of the paper is to highlight the basic definition of cyber terrorism, how often it is different from traditional terrorism, use of cyber terrorism, how cyber terrorism can be manipulated through various latest tools and techniques and how Islamic State (ISIS) is using cyber space to spread its message.

Keywords: Cyber space, cyber terrorism, cyber war, Islamic state, Islamic state online, cyber space manipulation, Islamic state social media

Introduction

The presence of terrorist organizations in cyberspace is not a new phenomenon as they have been showing their existence online since their very own inception. However, their reliance on cyberspace operations has tremendously increased since last two decades. The cyber terrorism threat has evolved into a multi-faceted and complex riddle where various ideological dogmas are turning the world into a cyber-war.

During 1998, half of thirty organizations which were designated as "Foreign Terrorist Organizations" under the US Effective Death Penalty Act of 1996 and US Anti-Terrorism maintained online presence through the developed websites.[1] By 2000, all terrorist groups had virtually set up their online presence.

The British scientist, Simon Singh states in "*The Code Book*":

* Zaheema Iqbal, M.Phil. student, International Relations, National Defense University, Islamabad
** Khurram Iqbal, Ph.D. Assistant Professor, Counter Terrorism, National Defence University, Islamabad
[1] Weimann, Gabriel. www. terror. net: How modern terrorism uses the Internet. Vol. 31. DIANE Publishing, 2004.

> It has been said that the First World War was the chemists' war, because the mustard gas and chlorine were employed for the first time, and that the Second World War was the physicists' war, because the atom bomb was detonated. Similarly, it has been argued that the Third World War would be the mathematicians' war, because mathematicians will have control over the next great weapon of war – information war.[2]

The cyber terrorism threat-prone landscape of ISIS is multi-layered and multi-dimensional. They have online presence and they are fighting this asymmetric war successfully. The paper will discuss the online recruitment procedure of the organization and how they manipulate the cyber space in order to achieve political gains. Much research has been done on conventional terrorism, its causes and aftermath. There are many researchers who researched and concluded that cyber terrorism may not pose serious threats in future and that it is more than a virtual game instead of physical terrorism. This paper attempts to highlight the misuse of cyber space by terrorist organizations focusing on Islamic State (IS) presence online.

Theoretical Framework

The study can be best described by the postmodern game theory as it is about opponents who wage war in unconventional situations and postmodern fashion. The game theory was enunciated by Emile Borel in 1921 which was further expanded by the mathematician John von Neumann in 1928 in 'a theory of parlor games'.[3]

The cyber terrorists and cyber experts both use tactics that are not common in traditional conflicts. The cyber terrorism is a war between two main protagonists of cyberspace. One looks towards manipulating the cyber space while other strives to protect it. The game theory best suits it as this theory is related to the study of power and control involving two or more actors with same or opposite interests.

Game theory offers a variety of new ideas and mechanism for defense and cyber-attacks. There is wide collection of perspectives for mocking-up the cyber warrior behavior but cyber hacker can change its behaviour according to the diversity of environment and community. In game theory, the cyber hackers use same methods of attack but during the attack, they keep on using different tactics to overcome or control the target. In cyber terrorism, a terrorist tries to gain more control over the object and they will be successful if they are able to cause more damage to the target. Game theory mostly deals with the conflict and cooperation between two or more actors. The actors are dependent on each other and they can be anyone i.e. an individual or a group of individuals, an agent or a group of agents. The theory tries to develop a basic structure to make people understand strategic scenarios.[4]

---

[2] Singh, Simon. The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography. Doubleday, 1999.
[3] Leonard, Robert J. "From parlor games to social science: von Neumann, Morgenstern, and the Creation of Game Theory 1928-1944." *Journal of economic literature* 33, No. 2 (1995): 730-761.
[4] Theodore I Turocy & Bernhard Von Stengel, "Game theory", CDAM Research Report, (2002): 14

There are three types of outcomes which are produced when applied on players. These outcomes are Nash equilibrium, zero-sum game, positive-sum game and negative-sum game.[5]

Nash equilibrium

John Nash gave the idea of Nash Equilibrium in 1950 which is the core concept of game theory. It is mostly used to envisage the outcome of strategic interaction of two agents in given circumstances. They both play their part and primary actions.[6] The central idea of this theory is to recommend a strategy to each player which cannot be improved upon by the player unilaterally. Since both players in the game theory are rational so it becomes reasonable for each player to act upon and expect the opponent to follow the recommendations.[7]

Zero-Sum Game

The basic interests of actors are conflicting in zero-sum game. It is regardless of the final result, the victory of one opponent is balanced by the total number of losses by other opponent. This is known as zero sums because when one actor subtracts the total number of losses from total gains, the answer comes as zero. In this game, actor A can gain the outcome at the expense of actor B. At the same time, the losses and gains of both actors are sum to the same value.[8]

Positive-Sum Game and Negative-Sum Game

In positive-sum game, all actors can get benefited from the activities and actions of all players. This is regardless of the fact that who gets more benefit and who gets less benefit. In this situation, one actor loses but the other actor gains as a result. In negative-sum game, every actor gets affected by the actions taken by other actors. The actions taken by all actors affect each actor like one actor is gaining and other actor is losing and outcome would be overall loss.[9]

Historical Perspective of Cyber Terrorism

The cyber battlefield is real. It is a place where computers are used instead of gun, data pockets instead of bullets and firewalls are used instead of barbed wire.[10]

The global security today faces severe challenges and terrorism is one of them. The deliberated assassinations, destruction of man and material, mutilation of innocent, bombings, illegitimate and unlawful attacks against public and private infrastructure,

---

[5] Jonathan Matusitz, "A Postmodern Theory of Cyber-Terrorism: Game Theory", *Information Security Journal: A Global Perspective*, pp.273-281.
[6] A. Mehlmann, The Game's afoot! Game theory in Myth and Paradox, (Providence, RI: American Mathematical Society, 2000), p-21.
[7] Theodore I Turocy & Bernhard Von Stengel, "Game theory", CDAM Research Report, (2002): 15
[8] D. Fudenberg and J.Tirole, Game Theory, (Cambridge, MA: MIT Press, 1991), p.56.
[9] *Ibid.*
[10] Von Bredow, Wilfried, ed. Die Außenpolitik Kanadas. Springer-Verlag, 2013

killing of hostages and all other barbaric acts of killing have become a routine happening around the world. No one and nothing is safe from terrorist acts today. Such terrorism has posed serious threats to the international security and existence of states and international order. Since the fear of terrorism has imprisoned the whole world, international community is compelled to join hands together and wage war against it. The state-of-the-art technology, modern weaponry of mass destruction and most importantly a grave threat of cyber-terrorism may bring out a perilous situation in the world.[11]

There are many forms of terrorism specifically biological, nuclear and chemical terrorism. There is a hot debate among international community that whether cyber-terrorism is posing serious threats to international security or not. In order to better determine this, there is a strong need to understand cyber-terrorism.

Defining Cyber-Terrorism

A senior research fellow Barry Collin, at the Institute for Security and Intelligence in California first coined the term 'cyber-terrorism' in 1980s. He referred to cyber-terrorism as the linkage of cyber space and terrorism.[12] The working definition of cyber-terrorism was given by Mark Pollitt, special agent for FBI:

> Cyber-terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub national groups or clandestine agents.[13]

Politically motivated attacks that cause serious harm, such as severe economic hardship or sustained loss of power or water, might also be characterized as cyber-terrorism.[14]

There is no single definition of cyber terrorism yet which is universally accepted. There are a few definitions which focus on the intention of cyber terrorists, other focus on the manipulation of information technology by them. There are also a few security experts who define it in terms of the consolidated effect of any attack whereas a destructive and disruptive result, huge amount of fear can be generated similar to a traditional terrorist attack. Under such attacks, which can lead to the injury, death airplane crashes, extended power outrages, major loss of economy or water contamination are defined as cyber-terrorism.[15]

Few experts define cyber terrorism as a form of physical attack which can distort physical infrastructure's computerized nodes including electric power grid, telecommunication or internet without even touching a keyboard.[16]

---

[11] "Terrorism and Media: Abdication of Responsibility", (Jerusalem: The Jonathan Institute, 1979), P.37.
[12] Barry Collin, "The Future of Cyber-terrorism", Crime and Justice International, (March 1997), p. 15–18.
[13] Mark M. Pollitt, "Cyber-terrorism: Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, (October 1997), p. 285–289.
[14] *Ibid*.
[15] Serge Krasavin, "What is Cyberterrorism?", Computer Crime Research Center, (April, 2004), p.4-9
[16] Dan Verton, "A Definition of Cyber-terrorism", Computerworld, (August 11, 2003).

Few other assertions suggest cyber terrorism as a form of terrorism which has the ability to cut across all kinds of infrastructure protection and it cannot be executed without physical damage to the property because these two operate interdependently. To further explain this concept, it may be said that cyber terrorism is the use of computer as targets or weapons, used by politically motivated national or international individuals or a group of individuals or clandestine agents who cause or threaten violence and fear for influencing audience of a particular area. It may also be done to pressurize the government to amend in its policies as per the wish of these politically driven groups.[17] This definition encompasses all three models of cyber-terrorism i.e. electronic attack (EA), physical and computer network attack (CAN).[18]

There are two ways to explain cyber terrorism in general which are as follows:

1. *Effects-based*: This kind of cyber terrorism is done when the result of computer attacks are as destructive and disruptive as compared to traditional terrorism and create grave fear.

2. *Intend-based*: This kind of cyber terrorism is done when politically motivated or unlawful attacks are done to coerce the existing government to achieve a political objective or create great damage to economic infrastructure.[19]

Aim of Cyber Terrorism

The basic aim of cyber terrorism is most likely the same as of traditional terrorism i.e. "to create terror" among populace and for coercion of existing regime. Cyber terrorist activities include political, religious, financial, ideological and similar kind of acts. It is now transferred to the modern means of networking and creates serious threats to general public as well as private infrastructures.[20]

The History of Cyber-Terrorism

The history of cyber-terrorism is not so long as it has emerged in the past few decades as a global security threat. The targets of cyber-terrorism mainly consist of critical infrastructures i.e. electric power grids, transportation, telecommunications, oil and gas distribution, financial institutions and air traffic control system. A distributed denial of service (DDoS) network attack was launched in Feb 2000. The famous websites like CNN, eBay, Yahoo, ZDNet, Amazon and Datek were attacked. There were millions of individuals who were unable to access these websites which resulted in financial loss and decrease of sense of security offered by these websites.[21] In April 2001, a series of

[17] Brett Glanda, "Cyber-Terrorism and Information Security", (East Carolina University), pp.27-34.
[18] *Ibid.*
[19] HuaJian & Bapna Sanjay, "How Can we Deter Cyber Terrorism?", Information Security Journal, vol.21, No.2 (2012), 102-114(16)
[20] Jonathan, Matusitz, "Social Network Theory: A Comparative Analysis of the Jewish Revolt in Antiquity and the cyber Terrorism Incident over Kosovo", International Security Journal: A Global Perspective, vol. 20,No.1, (2011):34-43(39)
[21] Biegel, Stuart. Beyond Our Control? Controlling the Limits of Our Legal System in the Age of Cyber space. (New York: The MIT Press, 2003)

website defacements and cyber-attacks between USA and China occurred as a result of collision between USA surveillance plane and a Chinese aircraft.[22]

The extreme display of cyber-terrorism is the website defacement as it results in intimidation with ideological or political agenda. There are various examples of website defacements in past and present. Students from Korean university completely defaced Japanese websites to show their protest on the Japanese textbook content.[23] Furthermore, India-Pak conflicts and Palestine-Israel conflicts involved website defacement many a times.[24] In past, there was also an incident of hacking the website of National Science Foundation's Amundsen by Romanian cyber hackers.[25] In 2007, Russian cyber hackers were blamed for hacking into Estonia's network systems. This is quite challenging to counter the resourcefulness and adaptability of terrorists with changing technology and society. The kind of warfare needs to be recognized and responded to. In 2009, a report came into limelight stating that the US computer systems controlling power grid were manipulated by some foreign cyber terrorists by Chinese and Russians. The cyber-attacks which were launched against USA and S. Korea, included Pentagon, New York Stock, Department of Transportation, Treasury Secret Service and White House. The blame was on South Korea with no solid evidence.

Presence of Islamic State (ISIS) in Cyber Space

Islamic State (ISIS) is the only terrorist organization which has a strong and active social media presence. This is not merely online presence but it has come to a level to cause strong damage to its enemies through internet. Islamic State took over US CENTCOM and Newsweek twitter accounts in 2014. It spread the message to the world that not only ISIS cyber space capabilities are enhancing but are also showing new ways to target westerns sites. If we look into the cyber space presence of Islamic State (ISIS), we come to know that there are six distinct cyber divisions taking care of various social media areas. Below is the detailed overview of their six cyber divisions:

Caliphate Cyber Army (CCA)

Soon after the declaration of ISIS Caliphate, the first pro-ISIS cyber hacking group emerged. They hijacked USA CENTCOM and Newsweek's twitter accounts and this group named themselves as "Cyber Caliphate". In 2015, they targeted cyber-attacks on a large number of US websites including New Mexico, Albuquerque Journal face book and twitter profiles and a Fusion center in Tennessee. In order to expand and improve the brand, a British actor Junaid Hussain (a.k.a. Abu Hussain Al Britani) led it to make repute of ISIS online. He was formerly famous for 'TriCk' of TeaMp0isoN and served prison for hacking Tony Blair. He left UK and joined ISIS in 2013. Since he was equipped with relevant experience and technical knowledge ISIS utilized him for recruiting hackers and

[22] Keegan, Christopher. "Cyber-Terrorism Risk." Financial Executive 18.8 (Nov. 2002): 35-37
[23] Bronk, Chris. "Hacking the NationState: Security, Information Technology and Policies of Assurance." Information Security Journal: A Global Perspective 17.3 (2008): 132-142
[24] Keegan, Christopher. "Cyber-Terrorism Risk." Financial Executive 18.8 (Nov. 2002): 35-37.
[25] "The Case of the Hacked South Pole." Federal Bureau of Investigation Headline Archives. 23 Dec. 2016 .

spread their message across through internet.[26] He continued doing it until August 2015 when he was killed in drone attack in Raqqa. He also obtained a large number of sensitive data by compromising Fusion center. Though he was targeted and killed resulting in one slowing down of ISIS cyber activities, yet there are many other experts to take the seat of Hussain. After Hussain, Islamic State (ISIS) replaced Siful Haque Sujan, a British-educated computer expert and businessman and 31 year old Bangladeshi. He took Hussain's place and kept on hacking websites and social sites of US government until he was also killed in drone strike in December 2015. After he was killed, in order to continue Hussain's legacy, his wife Sally Jones began her late husband's mission. Today she maintains a violent and prolific social media presence of Islamic State (ISIS).[27]

Islamic State Hacking Division (ISHD)

The Islamic State Hacking Division was established in 2015. It appears to be affiliated with Cyber Caliphate. These two divisions were linked with the same thread by the strong leadership of Junaid Hussain. In late 2015, a citizen of Kosovo 'Ardit Ferizi' aka 'Th3Dir3ctorY, was alleged by the federal prosecutors for providing information to ISIS and hacking US service members identification numbers for the group. He was the leader of this hacking division and hacked a target resulting in theft of personal information of thousands of individuals. He then gave all this information to Junaid Hussain for public release. Hussain later on named it Islamic State hacking Division (ISHD).

He also hacked credit card information of many officials of state departments and also screenshot of conversation of US servicemen. Later the Islamic State Hacking Division (ISHD) accepted the hacking responsibility. It has also been observed during the research that ISHD remained unsuccessful in maintaining positive branding of ISIS.[28]

Islamic Cyber Army

In late 2015, a cyber-hackers group tweeted its official statement self-proclaiming them 'Islamic Cyber Army' (ICA). They said that the hackers' supporters of the Mujahedeen configure under the banner of unification in the name of Islamic Cyber [sic] Army to be …[the] working front against the Americans and their followers to support the ISLAMIC STATE Caliphate with all their forces in the field of e-jihad.[29]

They offered all cyber hackers and supporters of Islamic State (ISIS) to come together and join hands and work against crusaders electronically. Discussing their targets, they said that they will attack on every possible target including banks, airports, nuclear bases, recruited staff, infrastructure, and all other critical systems which are connected via internet. They also sent messages to the United States of America stating that 'we will not

[26] Farwell, James P. "The media strategy of ISIS." *Survival* 56, no. 6 (2014): 49-55.
[27] Spencer Ackerman, "US Central Command Twitter Account Hacked to Read 'I Love You Isis,'" The Guardian, January 12, 2015, http://www.theguardian. com/us-news/2015/jan/12/us-central-command-twitter-account-hackedisis- cyber-attack; Russell Berman, "The Hacking of Central Command," The Atlantic, January 12, 2015, http://www.theatlantic.com/politics/ archive/2016/12/central-command-accounts-are-hacked-centcom-isissoldiers- obama-cybersecurity-cybercaliphate/384442/.
[28] Eric Schmitt, "U.S. Intensifies Effort to Blunt ISIS' Message," New York Times, February 16, 2015.
[29] Weimann, Gabriel. "Terrorist Facebook: Terrorists and Online Social Networking." (2010): 19-29.

forget your war against Islam and killing of Sheikh-ul-Mujahedeen Osama. They have always focused on USA as their target and all alliances of USA. In their final threat, they declared:

> O disbelievers Your Fate will be killing, homelessness and misery know that…this [is] only the beginning and [we] will slaughter your necks over your land soon." And they ended their statement with: "America will not enjoy security and safety until we live it…[30]

This group was highly active on the fourteenth anniversary of 11 September attacks and they also issued a countdown saying "two hours and 24 hours left" with hashtags #Islamic Cyber Army and #America Under Attack.[31]

Under the same hashtag, they issued a statement on the eve of September 11 stating 'we are in your home Obama and we have stolen data of legislative personnel of White House.

Rabitat Al-Ansar (League of Supporters)

Rabitat Al-Ansar is basically a part of a much larger Islamic State (ISIS) supporter's media group named as the Media Front. It was not always considered as a cyber unit for Islamic State (ISIS). It has worked for the organization as a jihadist propaganda media unit for a year. The duties include releasing press releases, articles, data related to jihad, Jihadi material, data supporting ISIS's cause and all other material related to the Islamic State. This division is a highly pro-Islamic State. With growing community of the supporters of Islamic State, Rabitat Al-Ansar took responsibility for ostensible hacks. In March 2015, they issued a statement stating that soon they will launch a strong campaign under the hashtag #We Will Burn US Again.[32] This campaign included mass level distribution of English language-ISIS-propaganda material including videos showing US forces violent actions in Iraq. The group has also shown US nationals beheading videos and included them in campaign. The campaign not only included messages from well-known leaders to Americans but also sent messages to US people offering them to convert to Islam. The group has made several twitter accounts for mobilization and encouraging their online supporters.

Nonetheless, they also claimed to target American banks stating 'expect us'. This tweet had an image with this featuring a faceless individual bears ISIS' logo sitting at a laptop. The image also included text stating 'ELITE ISLAMIC STATE HACKERS'.[33]

---

[30] *Ibid.*
[31] Embar-Seddon, Ayn. "Cyberterrorism Are We Under Siege?." *American Behavioral Scientist* 45, no. 6 (2002): 1033-1043.
[32] "ISIS Produces a Promotional Video to Promote Lone Wolf Terrorist Attacks on the U.S., Canada and Europe," Shoebat Foundation, February 21, 2015, http://shoebat.com/2015/02/21/isis-produces-promotional-video-promotelone- wolf-terrorist-attacks-u-s-canada-europe/.
[33] "Unmasked: The Man behind Top Islamic State Twitter Account," Channel 4, December 11, 2014, http://www.channel4.com/news/unmasked-the-manbehind-top-islamic-state-twitter-account-shami-witness-mehdi.

Sons Caliphate Army (SCA)

This cyber terrorist group emerged in early 2016 named them as 'Sons Caliphate Army (SCA). Later on in April, they announced themselves as merger of Caliphate Cyber Army (CCA). They seem to be more inclined towards CCA as its creation announcement was advertised on CCA's telegram channel. Both of them have strong communication and coordination as compared to other cyber networks of Islamic State (ISIS). These two are also planning to constitute 'The United Cyber Caliphate'. In their first unprofessional video titled 'Flames of Ansar', they claimed to hack more than 15000 twitter accounts and face book accounts. They also claimed that they hijacked Twitter's official website and it remained unavailable for two hours.[34]

United Cyber Caliphate (UCC)

Caliphate Cyber Army (CCA) announced on April 4, the merger of several groups including Sons Caliphate Army (SCA), Kalashnikov e-security team, Caliphate Cyber Army (CCA), Ghost Caliphate section and creation of new cyber group called 'United Cyber Caliphate' (UCC). They claimed to be the experts on web-hacking tools and techniques and manipulation of cyber space. This announcement came soon after Caliphate Cyber Army (CCA) hacked a twitter account and announced it via private telegram channel. There have been other instances of deep coordination between various groups supporting Islamic State (ISIS). Soon after their merger, they defaced website of Indonesian Embassy in France showing a fallen Eiffel tower.

This is now an umbrella cyber organization under the patronage of which cyber terrorists are manipulating cyber space and this is at the moment strongest cyber terrorist's networks around the globe.

Techniques, Tactics & Procedures (TTPs)

It is still difficult to identify the tools, techniques and tactics of which Islamic State (ISIS) supporters are using. On the basis of cyber-attacks they launch, following can be figured out:

Islamic State hackers are observed coordinating their activities and campaigns in private using encrypted messages and communication platforms before launching a formal attack. In majority of cases, they pre-declare their intent to launch an attack using hashtags for galvanizing support from the audience.

It is also very important to note down the timings and dates of attack which are mostly at the time significant dates i.e. September 11 anniversaries. These dates and timings are highly important for Jihadi terrorists as they ensure full media coverage and security agitation which allow them to get huge traffic on social media.

[34] J. M. Berger and Jonathan Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Brookings Project on U.S. Relations with the Islamic World, Analysis Paper No. 20, March 2015.

With regards to communication techniques and tools, it has also been observed that they use online encrypted platforms such as Telegram and Surespot. It is still difficult to say whether these tools are in-house developed or custom-made tools but on the basis of their attacks, these tools may be divided into two groups; hacking tools which are used to penetrate into a computer system externally resulting in compromising the system from inside. The second group of hacking tools is easily taken from publicly open source as they can be used successfully. For creating proprietary tools, it needs hard efforts and resources to develop a private tools kit which should be equal or better than already available tools.

The Future of ISIS's Cyber Capabilities

There is no doubt in it that Islamic State cyber capabilities have grown tremendously since its inception and it has the largest network of cyber hackers and cyber terrorists who are constantly busy in launching attacks on American and European targets. They will keep on sending DDoS attacks and keep on defacing websites. It is also true that they are working on improving their cyber capabilities by making advanced tools and infiltrating into others' system without any risk. It also depends largely on the cyber hackers' ability to bring top notch technological techniques with modern equipment as Junaid Hussain has set the precedence for all to follow.

Manipulation of Cyber Space

Islamic State's social media strategy is a 'double-edged sword' according to Farwell.[35] As IS is getting successful in gaining territory though displacements, violence and warfare, the social media strategy remains active and based on sophisticated tools.

Publicity and Propaganda

The internet has provided huge gaps to terrorists for carrying out their operations and activities. It was a big question for terrorist groups to win publicity for their activities and causes. The transition from traditional media to modern media and latest technological tools has provided space to these terrorists for spreading their message across to capture attention of the audience. The Islamic State (IS) has not only increased its presence online by manipulating many social media platforms including Facebook and twitter but has also taken help from contact sharing mechanism like Just Paste and messaging apps like Surespot and Telegram. The important point for IS's online presence is that it did not centralize its social media unit. They spread across many continents. The organizations' closest peers are not only terrorist's groups but western brands, publishing outfits and marketing companies cooperate with IS in order to get more customers and to boost user engagements.[36] It not only provides them an opportunity to frame how different audiences perceive them but also gives them an open space to manipulate their enemies.[37]

---

[35] Farwell, James P. "The media strategy of ISIS." *Survival* 56, no. 6 (2014): 49-55.
[36] Winter, Charlie. "Documenting the virtual 'caliphate'." *Quilliam Foundation* (2015): 33.
[37] Conway, Maura. "Terrorism and the Internet: new media—new threat?." *Parliamentary Affairs* 59, no. 2 (2006): 283-298.

Recruitment and Mobilization

Cyber space has not only been used for raising funds but it has also been manipulated by Islamic State for getting recruits and for mobilizing supporters from one place to another.[38] The figures show that there are more than three thousand individuals from West who have left their countries and migrated to join ISIS. The internet space has provided an open space to the organization to connect to the world through social media. The initial communication converted to association which can lead to one-to-one chat using many social media tools such as Text Secure, Chat Secure and Red phone.[39] Besides, women have been recruited in ISIS more frequently. There is one very famous female jihadi website related to ISIS with the name of Umm Layth. It not only motivated girls from west to be radicalized but also motivated them to leave their houses and join ISIS. The three British girls had links with Umm Layth who were to join ISIS in Feb 2014.[40]

International Organizations to counter cyber terrorism

In today's world, cyber terrorism has become an international challenge and many international organizations have joined hands together to combat it. Due to dependency on physical infrastructure by mostly states, not all states are willing to share its cyber security information with other states. There are legal frameworks available but still there are loopholes in the system of cyber security in general. There are many pacts, treaties, agreements available against cyber insecurity.

Mutual Legal Assistance Treaties

Mutual Legal Assistance Treaties (MLATs) are treaties which usually apply to the list of activities related to cyber-crimes in which state parties need to help one another by providing evidence, information and other form of assistance when requested to ask. These agreements apply in situations where criminal has used cyber systems for carrying out their activities.[41] The agreements related to cyber-crimes and cyber security generally consist of treaties, universally accepted rules of conduct and the UN Charter and Geneva Conventions.

It is important to mention here that under the UN Charter, cyber-attacks or cyber exploitation which has same effects equivalent to that of physical use are considered 'armed attacks'. The U.N has reported to have this proposed as main principle while

---

[38] Weimann, Gabriel, and Katharina Von Knop. "Applying the notion of noise to countering online terrorism." *Studies in Conflict & Terrorism* 31, no. 10 (2008): 883-902.

[39] "ISIS Follower On Twitter Warns Against Using Kik Messenger Service 'When Chatting About Sensitive Jihadi Stuff,' Recommends Other Technologies, The Cyber and Jihad Lab, November 4, 2014. Accessed Jan 5, 2017.
http://cjlab.memri.org/lab-projects/tracking-jihadi-terrorist-use-of-social-media/isis-follower-on-twitter-warnsagainst-
using-kik-messenger-service-when-chatting-about-sensitive-jihadi-stuff-recommends-other-technologies/3

[40] Franz, A. & Shubert, A. (2015). "From Scottish teen to ISIS bride and recruiter: the Aqsa Mahmood story". CNN

[41] John Markoff, "Step Taken to End Impasse Over Cybersecurity Talks", (New York Times, July 17, 2010), A7, col. 1:

discussing with Russia and some other states.[42] So far international and many regional organizations have been very active in preparing legal framework on cybercrimes and cyber terrorism.

United Nations

There are various UN institutions which have provided tremendous efforts to combat cyber-crimes and cyber terrorism. The United Nations General Assembly Resolution in 2000 addressed many ways how states can struggle hard to combat the misuse of information technology or manipulation of cyber space. One of the resolutions 57/239 adopted in 2002 is all about setting up cyber security global culture.[43]

The Security Council's Counter-Terrorism Committee

The Security Council's Counter-Terrorism Committee in United Nations is the sole committee and main body to work for the promotion of collective response on counter-terrorism activities. It was established on 8th September 2001 in Resolution 1373 (2001) by the Security Council. It was basically adopted and executed after the 9/11 attacks in USA. It says that all actions, methods, principles and practices of cyber terrorism are against the purpose of United Nations and calls for all nations to gather and join hands against international threat.

G8 Group of States

In 1997, a subgroup on high level cyber-crimes, the G8 Group of States was set up. It has ten core principles for countering computer related crimes. The purpose of its establishment was to ensure that no terrorist can receive safe havens in any state of the world.[44]

Asian Pacific Economic Cooperation (APEC)

The leaders and ministers of Asian Pacific Economic Cooperation (APEC) have made a commitment to try to implement a comprehensive list of rules and laws related to cyber-crimes, cyber security. These endeavors were consistent with the Council of European Convention on cyber-crimes and United Nations General Assembly Resolution. In 2003, Counter-Terrorism Action Plan was also made and Counter Terrorism Task Force (CTTF) was set up in 2003.[45]

---

[42] *Ibid*.
[43] *The resolution was adopted by the General Assembly on December 4, 2000.*
[44] G8 Information Centre, University of Toronto, Canada, see <www.g7.utoronto.ca>
[45] *Makarim Wibisono, Ambassador and Chair CTTF: APEC´s Strategy to Support International Law Enforcement Cooperation to Counter Terrorism in the Asia-Pacific Region, (Bali 2004).*

Organization of American States (OAS)

This organization was made in 1999 and it consists of experts from government. The main purpose of this organization was to prepare inter-American legal structure for countering cyber-terrorism. It was officially taken up in 2002 after 9/11 incident.[46]

Conclusion

Whenever a cyber-exploitation or attack occurs between one or more groups or countries, this is not a consideration about how to combat in terms of reprisal or punishment. Rather focus is more on which criteria or technique to use for countermeasures. For the existing threat from Islamic State (ISIS) cyber experts, there is a strong requirement for deciding countermeasures for the attack, decision criteria from where to launch and determination of facing it, countering it with logical techniques and joining hands internationally to combat it.[47] We agree with the notion that there have been various incidents of cyber manipulation on many infrastructures which have also given rise to economic and social sufferings thus making it successful for the cyber terrorist.[48] To avoid cyber –terrorism, continuous development in security advancements tools and technologies cannot be shunned at any stage; treaties among nations related to cyber security prevention are also important, as time is not far when terrorists will be using cyber space to destroy or damage physical infrastructure through the manipulation of cyber space.[49]

The Islamic State cyber threat is undoubtedly the strongest of its kind and international organizations and all nations must come together on a serious note for the complete eradication of the cyber system of Islamic State, because Islamic State (ISIS) cyber experts are focused, professionals, top notch and they know when and how to hit the enemy. Their cyber terrorism strategies are two-fold and they are not only enhancing the sophistication of cyber techniques but considering cyber war as important as traditional warfare. It is also essential for all governments to narrow down the technological gaps related to cyber terrorism and cyber security. Seeking mutual information sharing among different countries for the solution of information security is also required. It should also be noted that existing laws for physical terrorism cannot be used for information technology environment. Thus, there is a dire need for the legal framework to be made for implementation on cyber terrorism activities.[50]

---

[46] Samuel M. Witten, Deputy Legal Adviser, US Dept. of State: *Testimony before the Committee on Foreign Relations*, (US Senate, June 17, 2004).
[47] J. T.Kim, S. Y.Park, and T. Hyun, "An Inquiry into International Countermeasures against Cyberterrorism", ICACT, (2005).
[48] V. Mitliaga, "Cyber-Terrorism: A Call for Governmental Action?", (2001). R.Nagpal, "Cyberterrorism in the Context of Globalization," Seminar on "Globalization and Human Rights", (2002).
[49] De Borchgrave, Arnaud, Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgerwood. Cyber threats and information security: meeting the 21st century challenge. Center for Strategic & International Studies, (2001).
[50] M.M.Pollitt, "Cyber-terrorism - Fact or Fancy?", (FBI Laboratory, 2003).