Terrorist Threat on Internet: Current Global Response

Afeera Firdous*

Abstract

This paper differentiates between conceptual foundations of cyberterrorism and terrorist activities on the internet. The changed nature of terrorist threats on the Internet such as emergence of lone wolf attackers, advent of new techniques like narrowcasting and extensive use of social media for online terror financing and e-marketing have widened its effect on the common man. This changed nature of threat makes it important to understand the ways and techniques terrorists are using on the internet to attract the masses. This paper also describes the efforts of international or regional organizations and global social media companies against the terrorist use of the internet. Finally, this study assesses the remaining gaps in the current global counter-measures against terrorism in cyberspace because of which terrorist organizations and individual terrorist are still successful in their heinous purposes.

Keywords

Terrorism, Internet, Cyberspace, ISIS, UN, Google, Twitter, Facebook.

* Afeera Firdous is a Research Assistant at the Center for International Strategic Studies (CISS) Islamabad.

Introduction

Cyberspace has become a defining facet of today's world. The US Department of Defence described it as a universal domain in the overall information environment. It includes associated and inter-connected networks and infrastructure system. A vast range of technologies are part of it such as the Internet system, telecommunication networks, computer systems, installed processors and controllers. A fiction writer, William Gibson, coined the term "cyberspace" for the first time in his novel Neuromencer, in 1984.[1] Presently, cyberspace is evolving as another conflict domain in military doctrines. However, in the broader social content, it is described as a significant foundation in which the complete ecosystem and industries are evolving together.[2] Cyberspace is also increasingly being used by terrorists and extremist elements to promote their agenda. Use of cyberspace by extremists and terrorists is attributable to two factors. First, the instant communication made available by this technology solely dependent on user-generated content and the second, the awareness that the given technology can be exploited and used as an instrument for attaining their objectives.

Initially, the terms "terrorism in cyberspace" (use of virtual spaces or internet for terrorist purposes) and "cyberterrorism" were used interchangeably. However, these terms have different implications. The term cyberterrorism was first employed by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, in 1997. He defined cyberterrorism as the conjunction of "cybernetics and terrorism".[3] In her testimony to the House Armed Services Committee Special Oversight Panel on Terrorism, Professor Dorothy E. Denning, Director of Georgetown Institute for Information Assurance, stated that cyberterrorism is the "convergence of terrorism and cyberspace".[4] In general, it is assumed as an attack and/or risk of attack on computer systems and the data saved in it, to impede

and force a government and/or people to certain action(s) for political and/or social gains. James A. Lewis, Senior Vice President of Centre for Strategic and International Studies (CSIS), defined cyberterrorism as the use of computer network tools to crash and stop the critical national infrastructure to threaten a government and its civilian population by terrorists.[5]

In contrast, numerous studies have examined terrorists' diverse usages of the internet.[6] The known terrorist-related usages of online platforms are for psychological warfare, propaganda, online indoctrination, recruitment and mobilization, data mining, virtual training, cyber-planning and coordination, and fund raising. Studies have documented numerous categories of terrorists' use of the internet. Currently, terrorists are using internet for propaganda, fund raising, recruitment or planning, but there is not a single reported incident of cyber-attack (cyberterrorism) against any country or government by terrorists; whereas, with technological advancements and funds available to them such attacks cannot be ruled out in future.

The purpose of this study is to analyze the changing nature of terrorists' threat with advancement and easy availability of technology. While discussing the international security issues, apart from nation states, international organizations also form a significant part of the process. This paper will examine how international organizations, global IT and social media companies are responding to prevailing threat of terrorism on the internet. Also, it will evaluate the extent to which the current response is able to tackle the problem.

Changed Nature of Threat

Nature and scope of extremism and terrorism has transformed with the evolution of the internet and its various platforms. Terrorism and internet, in fact, complement each other in several

ways. Internet has developed into a supportive medium for extremist and terrorist organizations, groups and individuals to spread their agenda and to communicate within the groups, and with their followers. It has led to the emergence of innovative terrorist practices such as lone wolves on the internet, narrowcasting on the internet, online terror financing and terror through social media.

Terrorism perpetrated by individuals, known as lone wolves, is the fastest growing phenomenon of terrorism, online and on ground. Lone wolf terrorists are being hired, radicalized, educated and trained by others on different online platforms like Facebook, Twitter, chat room, YouTube etc. There is a complete online guide accessible for an inspired lone wolf who can learn anything from constructing a home-made bomb to maps and vicinity of the target. Gabriel Weimann said that an individual, lone wolf, is an open threat to the society who is radicalized through the internet and planning assaults in silence.[7]

Tom Metzger and Alex Curtis,[8] have made the term a Lone Wolf known in late 1990s. Ramon Spaaij defined it as "…terrorist attacks carried out by a person who operate individually, do not belong to an organized terrorist group or network, and whose modi operandi are conceived and directed by the individual without any direct outside command or hierarchy."[9] In contrast with a terrorist network, a Lone Wolf has some advantages: he/she certainly evades recognition and detection before and after the attacks because he/she generally does not expose his/her preference or liking as well as plans. According to Marc Sageman, most of the lone wolves participate in online forums. He argues that the internet gave a ground to these disconnected and dispersed people to interact and dialogue which was not available before. Through online mediums, individuals reluctant about sharing their radical opinions in person can simply find compatible people on online forums.[10] The 2010 Stockholm suicide bomber,

Taimour Abdul Wahab al-Abdaly,[11] and 2011 Norway attacker, Anders Behring Breivik,[12] are apt examples of lone wolf terrorism. Al-Qaida is one of the prominent terrorist organizations which started promoting lone wolf terrorism from the early years of twenty-first century.[13]

Narrowcasting is the spread of ideas and content limited to a particular set of audience. In post-modernist thinking mass audience is nonexistent. In general, narrowcasting aims to target an explicit portion of the community based on values system, social inclinations, demographic characteristics, and sex and age.[14] Terrorists have understood and recognized its significance in internet domain and, therefore, are using it effectively. Terrorists' websites, blogs, magazines and pages of Facebook incredibly focuses on the segments for children and women these days. Islamic State of Iraq and Syria (IS) and Al-Qaeda have been using digital publications/booklets for women and teenagers, stories and online video-games for children as tools to target large online audience.[15]

Terrorist groups and their supporters mostly are connected to different communities in different parts of the world by using forums like Facebook, Twitter, Myspace, Second Life, or their counterparts in other languages. Anthony Bergin, an Australian expert on counterterrorism, says that terrorists and extremists use such youth-dominated forums as a tool for propaganda and recruitment "in the same way a pedophile might look at those sites to potentially groom would-be victims."[16] ISIS remained successful in recruiting hundreds of Europeans, South East Asians and North Americans as ISIS fighters in Syria and Iraq is the proof of an accomplished narrowcasting strategy. A strategic, security, intelligence service institute, Soufan Group, reported that out of 12000 foreign fighters of ISIS in Syria, during 2013-2016, 3000 belonged to Western countries.[17]

'Social Media', also called as 'new media' is the wonders of twenty-first century. But extremism and terrorism are certainly its darkest sides. The case of young medical college student in Pakistan's city of Hyderabad, Noureen Laghari, is a recent example of social media preys of terrorists.[18] Noreen Laghari abandoned her home and education at university to join a terrorist group. She was, later, arrested from Lahore by the security agencies in an interception to prevent the terrorist attacks planned during Easter celebrations. For modern terrorist organizations like ISIS, social media platform is the cheapest and quickest way to propagate its ideology and radicalize youth. Uzbek immigrant, Sayfullo Saipov, was charged with the death of eight persons after driving a truck onto them in Manhattan on October 31, 2017. He was also suspected of providing substantial support and resources to ISIS. The latter charge stemmed from the discovery of ninety ISIS publicity videos on his mobile-phone which he confessed had motivated him to commit the killings.[19]

Online Terror Financing and E-Marketing

Online platforms have increasingly become key forums for receiving monetary assistances and funds; and advertising their products to get profit/revenues by the terrorist organizations. Currently, many terror groups maintain and support different websites for digital marketing of their products. ISIS and other terrorist organizations like Al-Qaeda have more experience, in exploiting the online platforms for financing, than other terrorist organizations. A young British man, Younis Tsouli, with online identity of Irhabi 007 (Terrorist 007), abetted terrorist organizations with his activities on internet for financing[20]. Tsouli started posting videos describing terrorist campaigns on several online forums. Leaders of Al-Qaeda in Iraq (AQI) were fascinated by his computer skills and motivation. As the ties between Al-Qaeda in Iraq and Irhabi 007 grew, they started feeding

propaganda videos to Irhabi 007 to post on online platforms.[21]Tsouli and his associate, Tariq al-Daour, also commenced stealing online credit card numbers, procuring these through many online platforms, such as Card planet.[22] When both of them were detained by the authorities, they had embezzled 37,000 online credit card numbers to make around $3.5 million.[23]

The online operations of charitable organization and Non-Governmental Organizations (NGOs) are also suspected to be linked to the terrorist organizations to fund these networks globally. According to the Paris-based Financial Action Task Force, "the misuse of nonprofit organizations for the financing of terrorism is coming to be recognized as a crucial weak point in the global struggle to stop such funding at its source."[24]

Use of Internet for Terrorist Purposes

The changed nature and scope of technology has not only affected an individual's life, but in fact it has absolutely transformed activities of societies, nation-states, and all actors on the global stage including terrorist organizations. Revolution in IT sector has also given opportunities to terrorists and followers to re-consider and re-establish their impact. Currently, conducting cyber-attack on states' infrastructure is not the prime agenda of terrorist groups, perhaps because of lack of technologies expertise, but the future threat still persists as highlighted in Federal Bureau of Investigation's (FBI) report about call for jihad against American critical infrastructure in form of cyber-attacks.[25] Major possible uses of internet are discussed in subsequent paragraphs.

Propaganda

Freedom of speech is a basic human right (offline and online), according to Article 19 of Universal Declaration of Human Rights, which later became the foundation stone for International Human

Rights Law. This right is, however, being misused by extremists and terrorists, who use internet platforms for promoting their agenda. Common theme of terrorists' online propaganda is promotion of violence. Cyberspace, as a domain, is not only being used as a medium to publically circulate the content but now it is a tool to incite, radicalize and recruit masses especially the youth. Apart from the public social media platforms, terrorists also use other forums like password-protected websites and limited access chat-rooms for *covert recruitment*.[26] For instance, an Austrian teenage boy Lloyd Gunton, claimed to be a soldier of ISIS, was found guilty of plotting ISIS-inspired terror attack.[27] Later, investigators found that Gunton was a prey of ISIS online propaganda.

Radicalization

Terrorists, individuals and organizations, have become proficient in using cyberspace as an instrument in the whole radicalization process. A new research by Policy Exchange, a think tank, revealed that ISIS and other terrorist groups are winning an ongoing "netwar" against government authorities who are trying to stop the spread of extremist material online.[28] Roshonara Choudhry's case is the example of online radicalization. She was the only British woman sentenced for a brutal terrorist attack. As a young university student in 2010, she knifed a Member of Parliament, after following Al-Awlaki-inspired videos on social media. [29] Contemporary radicalization theories describe Roshanara Choudhry as a "pure lone wolf," target of internet radicalization, without direct interaction with any terrorist group.

Virtual or E-Training of Terror

Currently, terrorists manipulate cyberspace not only as a tool for radicalizing the users, it has also become a forum to spread training of extremism and terrorism through different means such

as audios, videos, online magazines, presentations, illustrations and online tutorials etc. As Al-Qaeda publishes a digital magazine called *Inspire.* The objective of the magazine is to offer training facility to online potential recruits.[30]

Planning

In the modern era of social media, users innocuously share a bit of sensitive information online, where the weaknesses shared by people are ill-used by terrorists. At present, terrorists are using online applications like Google Earth and huge bulk of data present on such apps for planning their agendas.[31] Over the years, terrorist activities and operations have developed into more sophisticated methods in employing and manipulating communication technologies especially the internet. For example, the method of using 'Dead Drop' digital messages to share and disseminate terror plans in closed groups.[32] Dead drop refers to generating a 'draft message' in an e-mail account, which can be accessed by any internet terminal around the world by a person having password of that particular account.

Countermeasures: International and Regional Organizations

Terrorism on the internet has become a global threat, which needs a cohesive and coordinated response from countries, as well as international and regional organizations. United Nations (UN) is a viable forum for sharing of good practices worldwide. Working in this regard, it can be divided into two levels: international and regional. Some frameworks or resolutions deal with the issues of terror financing and others with recruitment, incitement and glorification of terrorist acts and using internet to spread counter strategies against terrorism.

International Organizations

The United Nations Security Council (UNSC) Resolution 1373[33] was adopted on September 28, 2001, and the other UN Resolution 1566[34] was adopted on October 8, 2004, under Chapter 7 of Charter of the UN to fight and counter terrorist acts in all of its types and practices. Both these resolutions aim at ceasing and abolishing the financing and funding of terrorism, recruitment by terrorist organizations and refraining from supporting any active or passive terrorist activity. On September 14, 2005, the Security Council adopted one more significant resolution, UNSCR 1624, which prevents the 'incitement and glorification of terrorism'.[35] UNSCR 1624 can be applied to offline and online terrorist activities.

Furthermore, understanding the need of the hour, United Nations General Assembly (UNGA) discussed UN Global Counter-Terrorism Strategy.[36] UNGCTS, later, was approved by all members. The strategy pursued all members to criticize, condemn and take firm actions to counter all types of terrorist activities. It directed countries, member of UN, to put up joint and coordinated measures in fighting terrorism on the internet. UN strategy also suggested that member states employ internet as a tool to counter this menace. After more deliberations, in December 2010, UNSC adopted Resolution 1962 to re-enforce and extend UN's resolve against terrorism.[37] Resolution 1962 particularly focused on terrorist propaganda for recruiting and inciting masses.

Nevertheless, no international resolution or agreement exclusively aims at suppressing the online terrorist activities. Another resolution by UNGA, Resolution 65/230,[38] was adopted in December 2010. Resolution 65/230 agreed upon the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Developments in a Changing World.[39] It paved the way to

formation of an inter-governmental expert group to organize comprehensive research projects to assess the consequences of use of internet for terrorist and criminal purposes.

Regional Organizations

Counter-terrorism is one of the key focuses of regional alliance, Shanghai Cooperation Organization (SCO). In 2011, SCO has officially proposed and accepted the Code of Conduct for International Security, which was revised, later, in 2015.[40] The first draft of the Code of Conduct was proposed by three-member states, China, Russia, and Tajikistan. SCO's Code of Conduct for International Security has features which demands of member states to develop common standards for 'information security, stability and interoperability in the cyberspace'. Article 4 of SCO's Code of Conduct binds the member states to cooperate for curbing cybercrime and terrorist acts as well as to counter hate speech.

The Council of Europe (COE) is another important regional forum which focuses on criminal acts in cyberspace. It adopted one and only multi-party legally binding framework, Convention of Cybercrime / Budapest Convention, on the issue of cybercrime in cyberspace, in 2001.

Another important regional mechanism, 2002/475/JHA, was adopted by European Union (EU) in July, 2002.[41]It assisted in coordinating counter-terror agendas in all the states parties of European Union. With the worrying rise of terrorist attacks in Europe, EU amended 2002/475/JHA in 2008 to stand against growing terrorist activities. The amended version 2008/919/JHA included clauses related to charging the offenses like incitement and terrorist propaganda, and delivering online bomb-making skills.[42] The new version of EU law is not all internet inclusive but helps in coordinating with Council of Europe Convention on

Prevention of Terrorism and also deals with online terrorist activities.

South Asian Association for Regional Cooperation (SAARC) is not an active regional body these days. Moreover, as of now, it has no framework to coordinate and counter the terrorist activities in its member states. In 1987, Regional Convention on Suppression of Terrorism of SAARC was approved to counter terrorism in the region. It is aimed at combating all types of terrorism and its facilitators. Subsequently, neither SAARC worked on specific issues related to online terrorist activities nor agreed on a specific internet related anti-terrorism framework. However, based on Regional Convention on Suppression of Terrorism, this can be applied to the cases related to online terrorism.

These measures, taken by regional and international organizations, are important to develop consensus of participating countries about terrorist activities on internet. But most of these agreements are legally non-binding and not obligatory on the states parties to take national legal measures in order to implement agreements. So most of these agreements are important/vital on paper but contribute little to the prevention of terrorism activities on the internet.

Counter Mechanisms by Global Social Media Giants

In recent years, social media networks have become increasingly more significant in shaping up the outlooks and approaches of the common people towards specific issues. Political and non-political forces have grabbed bigger roles in states' matters through social media influence. As terrorist activities grew in different parts of the world, extremist and terrorist organizations also realized the importance and impact and reach of social media and internet. These tools then became crucial for their propaganda, mobilization and other activities. NATO StratCom Center of Excellence

examined the case studies of Russians and Daesh of their internet and social media activities. The COE, on the basis of evaluation of data, established that apart from Russians, terrorist organizations have also modified their mode of operation. They are efficiently using new information technologies to influence the target audience.[43]As the use of internet and social media by terrorists grew with escalating impact on society, the critics forced social media corporations for safer online mediums. EU has also developed and adopted a law to force international social media firms to make extensive efforts to counter extremist and terrorist propaganda on the internet.[44] Some of the cases are discussed here.

International social media firms started their services with the laudable objective of making available freedom of expression and freedom of speech platforms for the common man but they could not insulate these from the spread of extremist and terrorist thought. Due to increase in extremist content on social media, the huge Silicon Valley corporations had to face criticism on the content available on these sites. Responding to the criticism, big firms from Silicon Valley; Google (YouTube), Facebook (WhatsApp), Twitter, Microsoft etc. have organized a coordinated forum, Global Internet Forum to Combat Terrorism (GIFCT)[45] with the vision to prevent terrorists from using their platforms. These big Silicon Valley companies vowed to adopt several counter mechanisms to cope with issues related to accounts check, practice of artificial intelligence (AI) to locate terrorist content, hiring additional moderator to check content, backup counter-speech, development of a coordinated database of hashtags for terrorists' image recognition etc. As the companies share the new platform GIFCT, they will cooperate with each other for content recognition, machine learning, and defining the transparency rules for elimination of extremist content and hate speech from their respective sites. In June 2018, the member firms of GIFCT have

celebrated the first year of successful joint operations. The ongoing work needs to be acknowledged, but substantial issues still remain unchallenged.[46]

In 2016, Facebook along with other three IT giants, Microsoft, Twitter and Google (YouTube), revealed that all these firms will coordinate with each other to build shared data-base to eliminate terrorist content from their relevant online platforms.[47] In a joint statement, these corporations stated that a common database of 'hash tags' will be developed and shared amongst all these firms which will assist to locate terrorism-related content on online platforms. Official statement indicated that the database will be developed and functionalized by 2017. All collaborating companies anticipated that their efforts will get positive response as other IT companies will also join them in future.

In mid-2017, the Guardian newspaper acquired some internal files of Facebook through anonymous sources. These documents exposed the intricate policy and techniques of social media corporations to counter online extremism and terrorism.[48] They revealed that social media companies ordered the content moderators to memorize the list of 600 terrorist containing their names and pictures. According to these files, Facebook report had identified more than 1300 posts on their social site as 'credible terrorist threat' in a single month and stated that it helped to identify some new terrorist groups and individuals which is considered a huge success. Facebook also invested in AI tools for 'proactive screening' to detect and eliminate terrorist content prior to its circulation on the forum. Besides all these advancements, some critics say that social media companies are still behind in countering online terrorism and extremism as terrorist have also developed advanced techniques and methods to by-pass these efforts.[49]

Google has also adopted more substantial and resilient stance, especially on use of YouTube channels. It affirmed that the firm will give warning on the issue of terrorist or extremist videos; those video will neither be paid nor the company will recommend these videos to other users.[50] Google (YouTube) has put its policy in the following four parameters to respond to terrorist or extremist content.[51]

- Additional resources to build their AI tools.
- Engaging more experts for Trusted Flagger Program of YouTube. Google planned to assist further 50 non-governmental organizations to existing planned 63 organizations for the program.
- Strong and rigid response to speculative and ambiguous videos which raise cautions according to YouTube's policy.
- Work along with Jigsaw to employ ad-targeting strategy against likely ISIS targeted youth to alter their minds from joining terrorist groups.

About its plan to counter terrorism, Facebook has shared its strategy and disclosed many ways in which this social media company uses Artificial Intelligence (AI) to fight the terrorists' activities. Facebook also stated that their recent efforts are particularly directed against Islamic State, AL-Qaeda and their supporters. The company is looking to utilize technology to combat other terrorist organizations' activities in the future, with about 150 staff members focusing on finding online terrorism.[52] Additionally, it stated that scrutinizing the forum (Facebook) is really a complicated task when around 2 billion users access it worldwide and write in more than 80 languages. The strategy, shared by it, uses different ways showing how Facebook is trying to offset the terrorist activities.[53]These may be summarized as follows.

- Image identification tools to recognize images on Facebook to mark and stop circulating extremist and terrorist propaganda images.
- Trials of language understanding methods and systems to apply AI to detect terrorist content in text on social media sites.
- Using algorithms to identify and trace extremist and terrorist groups and their extended connections (friends and followers).
- Usage of AI tools to detect and stop 'repeat crooks' which plays an important role in flowing terrorists' propaganda.
- Observing and monitoring extremist and terrorist activities not only on Facebook but also on other Facebook-owned apps like WhatsApp and Instagram.

In early 2017, Facebook founder Mark Zuckerberg outlined a plan to let AI software review content posted on the social network to spot violent and terrorist activities.[54] Later in November 2017, Facebook claimed that the efforts to use AI and other automated techniques to delete terrorism-related posts are bearing fruit.[55] Facebook also referred to text-based machine learning, in which software is trained over time to detect posts which are most likely to be of concern by analyzing factors such as the frequency with which certain words and phrases appear. Facebook announced that once a piece of terror content was flagged as such, it removed 83% of the material and any subsequently uploaded copies within an hour of these being posted. In a big move against extremist and terrorist content, Facebook recently asserted that it removed or flagged 1.9 million pieces of content linked to al-Qaeda or ISIS in the first part of 2018, twice as much as in the previous quarter.[56]

Micro-blogging social media site, Twitter, confronts different challenges in this regard. The company has a past of advocating freedom of speech and anonymity through the Internet for a long

time, whereas Facebook and Google have pressed for real names. Different research studies[57] have revealed that Twitter is one of the most popular ISIS instruments for disseminating propaganda and directing people to private messaging applications, like Telegram. In May 2017, legal action was initiated by the families of the victims of San Bernardino's attack, as they believed that Twitter had knowingly supported the Islamic State and its extremist agenda.[58] Clearly, linked accounts with ISIS were deleted and Twitter blocked 376,890 accounts for counter-terrorism violations only in the second half of 2016.[59] While Twitter's transparency report in May 2018 stated that the company also removed more than 270,000 accounts around the world for promoting terrorism in the second half of 2017.[60]

Conclusion

Approximately 47% of the world is now connected to the internet, as compared to 1% in 1995. One billion online users existed in 2005 and the number may increase to five billion very soon. Information technology has changed its nature rapidly and extended its scope so widely that its impact has become discernible on individuals, society, state, politics, environment, and even on psychological issues in a short span of time. Increased number of online platforms and users has also led to ease of access to terrorists to use these mediums for the propagation of their ideology and attracting new recruits. The scale of impact has widened with passing years. States, international organizations, IT and social media companies are presently working to deal with the issue of terrorists' presence and use of internet in a way that is not yet well coordinated. Countering the menace of terrorism in cyberspace demands a comprehensive and finely tuned coordinated strategy in order to effectively deal with this menace.

Major focus of terrorist activities on the internet remained on indoctrination, incitement for violence (propaganda), recruitment, terror financing, e-marketing rather than conducting cyber-attacks against adversaries. But terrorist threat on the internet has spread so widely that countries as well as IT companies realized the need to develop a coordinated effort in order to effectively cope with the complexity of the problem, with multilateral agreements. The problem, however also, lies in the nature of these agreements as well, because most of regional and international counter-measures against terrorist threat on the internet are non-binary in nature. So the countries do not feel any compulsion to adopt agreed measures on a national level.

One problem still being faced by different platforms on the internet is that, if a terrorist group or individual is blocked on one forum, it might easily move to some other forum. A terrorist can exploit one platform by switching user profile, account, page or channel many times. To counter this, GIFCT members have generated and shared a database of hashes or unique digital fingerprints to follow and block online activity. But this has not eliminated the problem completely. Regarding the disruptions of online accounts (especially on Twitter), terrorists and their followers have started to bypass content blocking technology by "out-linking" the content to other platforms. As GIFCT consists of a limited number of IT and social media companies, terrorists are therefore effectively manipulating smaller companies' lack of expertise and resources.

ISIS has also moved its activities on platforms which provide more covert methods of communication such as cloud-based end-to-end encryption like Telegram and WhatsApp. The end-to-end encryption stops the intervention of third party. Terrorists have also relocated their websites and activity to Darknet, which is not easily accessible and have closed groups of audience and participants using special encryption software. Henry Jackson

Society has warned that Darknet platforms have become virtual safe-havens for terrorist organizations for communication and planning.

Another problem with the initiatives taken by international organizations is that their agreements or memorandums are not legally binding to the states. Developing countries do not have technical expertise to contain online activity of terrorists. International organizations like International Telecommunication Union (ITU) therefore would need to assist small and developing countries to counter terrorists' online activity through information sharing and technical support.

Endnotes

[1]Daniel Punday, "The Narrative Construction of Cyberspace: Reading Neuromence, Reading Cyberspace Debates," *National Council of Teachers of English* 63, no. 2 (November 2000), 194-213, http://extscifi.weebly.com/uploads/8/9/4/7/8947540/article39.pdf.

[2] David J. Beretz and Tim Stevenson, *Cyberspace and State: Towards a Strategy for Cyber Power* (London: Adelphi Books, 2011), 9.

[3] Barry Collin, "The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge," *Crime and Justice International* 13, no. 2 (March 1997), 15-18, http://www.crime-research.org/library/Cyberter.htm.

[44] Dorothy E. Denning, "Cyberterrorism: Testimony to the House Armed Services Committee Special Oversight Panel on Terrorism," *The Terrorism Research Center*, March 23, 2000, http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf.

[5]James Andrew Lewis, "Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats," *Center for Strategic and International Studies*, December 2002, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

[6]Aben Kaplan, "Terrorist and the Internet," *Council on Foreign Relations*, January 8, 2009, https://www.cfr.org/backgrounder/terrorists-and-internet, and

Hsinchum Chen, Sven Thoms, and Tianjun Fu, "Cyber Extremism in Web 2.0: An Exploratory Study of International Jihadist Groups," in *IEEE International Conference on Intelligence and Security Informatics*, Taiwan (June 2008), 98, https://ieeexplore.ieee.org/document/4565037/?part=1.

[7]Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Washington D.C.: Woodrow Wilson Center, 2015), 64.

[8] T. Metzger and A. Curtis, white supremacists, were part of White Aryan Resistance.

[9] Ramon Spaaij, *Lone Wolf Terrorism: Global Patterns, Motivations and Prevention* (New York: Springer, 2011), 16.

[10]Caryle Murphy, "Terrorism fight 'must shift to cyberspace' Saudi conference agrees," *The National*, January 27, 2011, https://www.thenational.ae/world/mena/terrorism-fight-must-shift-to-cyberspace-saudi-conference-agrees-1.384705.

[11] Jonathan Paige, "Stockholm suicide bomber: TaimourAbdulwahab al-Abdaly profile," *The Guardian*, December 12, 2010, https://www.theguardian.com/world/2010/dec/12/stockholm-suicide-bomber-profile.

[12] "Norway massacre: Anders Behring Breivik 'acted alone'," *BBC News*, July 25, 2011, https://www.bbc.com/news/world-europe-14266815.

[13] Gabriel Weimann, "Lone wolves in cyberspace," *Journal of Terrorism Research* 3, no. 2 (2012): 75-90.

[14] Gabriel Weimann, *New Terrorism and New Media* (Washington: Woodrow Wilson Centre Press, 2014), 3.

[15] Sara Monaci, "Explaining Islamic State's Media Strategy: A Transmedia Approach," *International Journal of Communications* 11 (2017): 2842-2860, http://ijoc.org/index.php/ijoc/article/viewFile/6975/2086.

[16] "Facebook Terrorism Investigation," *The Advertiser (Adelaide, Australia)*,

April 5, 2008, https://www.adelaidenow.com.au/news/facebook-terrorism-investigation/news-story/69a8ffd26505d472726348297a80f67f?sv=662b980c75ec55a62e7a84791e6e7e4a.

[17] Anne Aly, Stuart Macdonald, Lee Jarvis and Thomas Chen, *Violent Terrorism Online: New Perspectives on Terrorism and the Internet* (London and New York: Routledge, 2016), 53.

[18] "Female militant arrested from Lahore found to be 'ISIS-affiliated' Noreen," *The Nation* (Lahore), April 16, 2017, https://nation.com.pk/16-Apr-2017/female-militant-arrested-from-lahore-found-to-be-isis-affiliated-noreen.

[19] David Patrikarakos, "Social Media Networks Are the Handmaiden to Dangerous Propaganda," *Time*, November 2, 2017, http://time.com/5008076/nyc-terror-attack-isis-facebook-russia/.

[20] "Al Qaeda Today: The Evolving Terrorist Landscape," *FBI Stories*, September 28, 2007, https://archives.fbi.gov/archives/news/stories/2007/september/cfr092807.

[21] Gordon Corera, "The World's Most Wanted Cyber Jihadist," *BBC News*, January 16, 2008, http://news.bbc.co.uk/2/hi/americas/7191248.stm.

[22] "U.S. Secret Service's Operation Firewall Nets 28 Arrests," *US Secret Service*, press release, October 28, 2004, https://www.secretservice.gov/press/pub2304.pdf. These forums obtained the credit cards through various online scams and e-mail viruses. See: Brian Krebs, "Terrorism's Hook into Your Inbox," *Washington Post*, July 5, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html?noredirect=on.

[23] For example, one New Jersey woman described how she received an e-mail asking her to verify eBay account information, which she completed, including sensitive financial information. Al-Daour ended up with her credit card information. Brian Krebs, "Terrorism's Hook into Your Inbox," *Washington Post*, July 5, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html?noredirect=on.

[24] "Terrorist Financing," *Financial Action Task Force*, February 29, 2008, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.

[25] Jack Cloherty, "Al Qaeda video call for 'electronic jihad'," *ABC News*, May 22, 2012,

https://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875.

[26] Scott Gerwehr and Sarah Daly, "Al-Qaida: terrorist selection and recruitment", *The McGraw-Hill Homeland Security Handbook*, David Kamien, ed. (New York, McGraw-Hill, 2006), 83.

[27] Lizzie Dearden, "Teenage boy plotted Isis-inspired terror attack with knife and hammer in Cardiff," *The Independent*, November 28, 2017, https://www.independent.co.uk/news/uk/crime/isis-plot-cardiff-teenage-boy-terror-attack-knife-hammer-arrest-justin-bieber-online-radicalised-a8080886.html.

[28] Lizzie Dearden, "ISIS winning online war against Government's anti-terror efforts, new report warns," *The Independent*, September 19, 2017, https://www.independent.co.uk/news/uk/home-news/isis-winning-online-war-propaganda-extremist-material-radicalisation-report-facebook-twitter-social-a7954246.html.

[29]Vikram Dodd, "Roshonara Choudhry: I wanted to die … I wanted to be a martyr," *The Guardian*, November 4, 2010, https://www.theguardian.com/uk/2010/nov/04/stephen-timms-attack-roshonara-choudhry.

[30]Azmat Khan, "The Magazine that 'Inspired' the Boston Bombers," *Frontline*, April 30, 2013, https://www.pbs.org/wgbh/frontline/article/the-magazine-that-inspired-the-boston-bombers/.

[31] "Terrorism 2018: Al Qaeda uses Google Maps to plan a terrorist attack in new propaganda video that features a former Guantanamo prisoner," *Daily Mail*, April 21, 2018, http://www.dailymail.co.uk/news/article-5642361/Al-Qaeda-appears-use-Google-Maps-plan-terrorist-attack-new-propaganda-video.html.

[32]Eben Kaplan, "Terrorists and the Internet," *Council of Foreign Relations*, January 8, 2009, https://www.cfr.org/backgrounder/terrorists-and-internet.

[33] "UNSC Resolution 1373 (2001)," *United Nations DOC*, accessed on June 23, 2018, https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf.

[34] "UNSC Resolution 1566 (2004)," *United Nations*, accessed on June 23, 2018, https://www.un.org/ruleoflaw/files/n0454282.pdf.

[35]"UNSC Resolution 1624 (2005)," *United Nations*, September 14, 2005, https://www.un.org/press/en/2005/sc8496.doc.htm.

[36] "UN Global Counter Terrorism Strategy," *United Nations*, accessed on June 12, 2018, https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy.

[37] "UNSC Resolution 1962 (2010)," *United Nations*, accessed on June 24, 2018, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/702/23/PDF/N1070223.pdf?OpenElement.

[38] "UNGA Resolution 65/230," *United Nations*, June 24, 2018, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement.

[39] Resolution was adopted by the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Convention held in Salvador, Brazil from 12 to 19 April 2010, which addressed the need for member states to consider ways of fighting new form of crime, such as cybercrime.

[40] "SCO Code of Conduct for International Security," *NATO Cooperative Cyber Defense Centre of Excellence*, accessed on June 24, 2018, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[41] "Framework Decision 2002/475/JHA," *UNHCR*, accessed on June 27, 2018, http://www.refworld.org/docid/3f5342994.html.

[42] "Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on Combating Terrorism," *European Parliament*, September 5, 2014, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/general/docs/report_on_the_implementation_of_cfd_2008-919-jha_and_cfd_2002-475-jha_on_combating_terrorism_en.pdf.

[43]"New Trends in Social Media," *NATO Strategic Communications Center of Excellence*, December 2016, file:///C:/Users/Ms%20Afeera/Downloads/social_media_report_public_09dec.pdf.

[44] Samuel Gibbs, "Facebook and YouTube face tough new Laws on extremism and explicit videos," *The Guardian*, May 24, 2017, https://www.theguardian.com/technology/2017/may/24/facebook-youtube-tough-new-laws-extremist-explicit-video-europe.

[45] Sam Levin, "Tech Giants Team Up to Fight Extremism following Cries that They Allow Terrorism," *The Guardian*, Jun 26, 2017, https://www.theguardian.com/technology/2017/jun/26/google-facebook-counter-terrorism-online-extremism.

[46] Dave Lee, "Tech firms hail 'progress' on blocking terror," *BBC News*, June 8, 2018, https://www.bbc.com/news/technology-44408463?intlink_from_url=https://www.bbc.co.uk/news/topics/cvenzmgygl5t/counter-terrorism&link_location=live-reporting-correspondent.

[47]Rob Price, "Google, Facebook, Microsoft and Twitter are Working Together to Tackle Terrorist Propaganda," *Business-Insider*, December 6, 2016, http://www.businessinsider.com/r-web-giants-to-cooperate-on-removal-of-extremist-content-2016-12.

[48]Nick Hopkins, "Revealed: Facebook's internal rulebook on sex, terrorism and violence," *The Guardian*, May 21, 2017, https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence.

[49]. M. Berger, "How terrorists recruit online (and how to stop it)," *Brookings*, November 9, 2015, https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it/.

[50]Reuters Staff, "Google Tightens Measures to Remove Extremism Content on YouTube," *Reuters*, June 19, 2017, http://www.reuters.com/article/us-google-counterterrorism-idUSKBN19A096.

[51]Arjun Kharpal, "Google Outlines 4 Steps to Tackle Terrorist-related Content on YouTube," *CNBC*, June 19, 2017, https://www.cnbc.com/2017/06/19/google-youtube-tackles-terrorist-videos.html.

[52] Colin Lecher, "Facebook says it wants 'to be a hostile place for terrorists'," *The Verge*, June 15, 2017, https://www.theverge.com/2017/6/15/15811078/facebook-counter-terrorism-efforts.

[53]Rebecca Heilweil, "5 Ways Facebook Uses Artificial Intelligence to Counter Terrorism," *Forbes*, Jun 15, 2017, https://www.forbes.com/sites/rebeccaheilweil1/2017/06/15/5-ways-facebook-uses-artifical-intelligence-to-counter-terrorism/#9e391d649e69.

[54]"Facebook algorithms 'will identify terrorists'," *BBC News*, February 16, 2017, https://www.bbc.com/news/technology-38992657.

[55] "Facebook's AI wipes terrorism-related posts," *BBC News*, November 29, 2017, https://www.bbc.com/news/technology-42158045.

[56] Jeremy B. White, "Facebook says it removed or flagged 1.9 million pieces of terrorism-related content this year," *The Independent*, April 23, 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-terrorism-isis-alqaeda-content-removed-mark-zuckerberg-a8319001.html.

[57] Rick Gladstone and Vindu Goel, "ISIS is Adept on Twitter, Study Finds," *The New York Times*, March 5, 2015, https://www.nytimes.com/2015/03/06/world/middleeast/isis-is-skilled-on-twitter-using-thousands-of-accounts-study-says.html

[58] Matt Hamilton, "Families of San Bernardino attack victims accuse Facebook, Google and Twitter of aiding terrorism in lawsuit," *Los Angeles Times*, May 3, 2017, http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-tech-lawsuit-20170503-story.html.

[59] Selena Larson, "Twitter Suspends 377,000 accounts for Pro-terrorism Content," *CNN*, March 21, 2017, http://money.cnn.com/2017/03/21/technology/twitter-bans-terrorism-accounts/index.html.

[60] Press Association, "Twitter bans 270,000 accounts for 'promoting terrorism'," *The Guardian*, May 5, 2018, https://www.theguardian.com/technology/2018/apr/05/twitter-bans-270000-accounts-to-counter-terrorism-advocacy.