Counterterrorism in Cyberspace: Case Study of Pakistan

Afeera Firdous

Introduction

With the evolution of technology, the threat of terrorism has also grown as the internet has become a powerful medium for exploitation by terrorists. Internet's possible use by terrorists and hostile states has, therefore, attracted the attention of policymakers to critical issues associated with cyber-security, protection of individual and national data and threat of cyber weapons. Pakistan is one of those countries which have been victim of terrorism for almost two decades. Terrorist groups have primarily focused on showing gory pictures to spread their message of terror, apart from using traditional media to get coverage. However, there is dearth of information in public domain about the potential of terrorist groups to cause harm by using cyberspace and the level of control exercised by Pakistani authorities to restrain the activities of online terrorist groups.

This paper focuses on an analysis of how terrorist organizations in Pakistan are using internet to accomplish their goals - which includes but is not limited to propaganda, financing, mobilization, planning, execution, crowd-sourcing of ideas, and radicalization of vulnerable young people - and how Pakistan is handling this emerging threat of online terrorism.

Evolution of Threat Spectrum

The story of presence and use of internet by terrorists has just started being told. At present, the entire 61 organizations world-wide designated as Foreign Terrorist Organizations (FTOs)[1] under Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) of the US Congress, have multiple existence in cyberspace in form of websites, blogs, Facebook accounts and pages, Twitter accounts, YouTube channels and Telegram accounts etc. Currently, terrorist organizations are utilizing internet for communication and propaganda rather than cyber-attacks per se but cyber-terrorism is likely to be an attractive option for terrorists in future due to its potential to inflict wide spread destruction, psychological impact and media appeal.[2]

The evolution of internet and communication technology (ICT) made the beginning of the virtual space, identified as cyberspace,[3] possible. The US Department of Defense defines 'cyberspace' as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[4] In comparison the explanation of terrorism is not that straightforward. It is one of the most contested concepts among scholars. Stanley Hoffman has argued that many of us use the term but do not have clear idea of terrorism. Scholars call it violence directed in pursuit of political aim,[5] or politically motivated acts to inculcate fear in audience.[6]

The presence of modern terrorists in cyberspace is a primary feature of two key trends; first, democratization of communication by user-generated content and second, terrorists' expertise of use of this technology. Scholars have divided use of internet by terrorists in two categories; communicative and instrumental. Communicative use of cyberspace includes the spread of propaganda, launch of psychological warfare operations, securing inner communications and radicalizing potential recruits. In addition, instrumental use of the internet takes account of teaching and training of terrorists in the online spaces and establishment of "virtual training camps" for new recruits. Some of the usages of online platforms are psychological warfare, propaganda, online indoctrination, recruitment and mobilization, data mining, virtual training, cyber-planning and coordination, and fund raising. Emergence of new phenomena such as lone wolf terrorists, online terror financing and e-marketing, narrow-casting, and terror on social media have completely altered the nature of terror threat.

Online Counterterrorism Measures: An Overview

Terrorism on the internet is a universal problem and needs a cohesive response within the state and among nations. Countries have directed their endeavors to counter the threat of terrorism in cyberspace. Different regional and international forums like United Nations (UN), European Union (EU) and Shanghai Cooperation Organization (SCO) have also used their platforms for discussions of the threat and have chalked out good practices on this particular issue. But it is imperative to note that these recommendations are not obligatory for the member states to follow.

United Nations General Assembly (UNGA) has adopted UN Global Counter Terrorism Strategy in 2006. This strategy pursues the member states to systematize the efforts to neutralize all forms of terrorism on the internet and use the online spaces for counter narrative.[7] Counterterrorism is the core element on agenda of SCO apart from counter extremism and counter separatism. Article four of SCO Code of Conduct 2011 (amended in 2015) emphasizes on the need for cooperation against cybercrime and terrorist activities, including restricting hate speech by terrorists and their sympathizers.[8] In 2010, UK inaugurated 'Counter Terrorism Internet Referral Unit' to identify and report online commotions which support glorification or incitement of terrorist activities.[9] In 2015, France adopted legislation which stretched the government's surveillance on ground as well as online surveillance to counter the threat of terrorism.[10] Under enormous stress from critics, international IT companies and social media giants have also made efforts to counter terrorist content on different forums. The Silicon Valley firms; Facebook, Google (YouTube), Twitter and Microsoft, have shaped a shared platform, 'Global Internet Forum to Counter Terrorism'.[11] These companies avowed different measures, including permanent blocking of accounts, identification of extremist and terrorist content through using artificial intelligence (AI), using more content moderators, supporting "counter speech", and building a shared industry of database of hashtags to identify terrorist substance.[12]

Existing Online Terror Threats in Pakistan

Terrorism and ongoing war against terrorism is the most vital security challenge ever faced by Pakistan to its internal security. In the last one and half decades, Pakistan's attention has been focused on irregular war in Federally Administrated Tribal Areas (FATA), Balochistan and some urban areas of Karachi and Peshawar.

According to one assessment in 2016, internet users in Pakistan are more than 34 million.[13] With the tele-density of 72.41% (2016-17),[14] Pakistan has 5th highest growth rate in mobile connectivity in Asia. The improving internet handiness and operability have not only enhanced living standards, but also become part of the problem as well. Being a late entrant in cyberspace domain, Pakistan has not been giving the needed attention to online terrorism. National Counter Terrorism Authority (NACTA) has registered 66 terrorist groups as banned, yet almost all these organizations continue to use available online platforms. According to an extensive study carried out by Dawn newspaper about terrorist activities on Facebook, 41 out of the 65 proscribed groups in Pakistan are not only present on Facebook but also actively operate their pages, groups and individual profiles which are hundreds in number.[15]

Most recent example of Islamic State (ISIS) effective online reach in Pakistan came to light when a female medical student was detained in Lahore.[16] In early 2017, Naureen Laghari, a student at Liaqat

University of Medical and Health Sciences Jamshoro, disappeared from her university. In her last Facebook message to her brother, Naureen told she was safe and sound in 'the land of caliphate'.[17] On April 16, 2017, law enforcement agencies, in a statement, declared that a major terror attack on Easter has been thwarted in Lahore. Forces killed two of the terrorists and detained others which included Naureen Laghari. Later, Naureen speaking in a television interview said that she was approached by the terrorists on Facebook as she had been previously visiting Facebook pages of terrorist groups.[18] Another example is that of Ansar-ul-Sharia (ASP)[19], whose area of operation is mainly Karachi.[20] The group caught the attention, of law enforcement forces, after its failed assassination attempt on MQM leader Khuwaja Izhar-ul-Hassan. Security forces arrested educated ASP militants from different parts of the country. Enquiry revealed that the group members used 'code words'[21] and had developed a mobile app for highly secure communication network within the group.[22] These examples will help in understanding how the terrorist threat, through use of internet, has evolved in recent years.

Potential Threats

Emergence of 'lone wolf' attackers is a rapidly emerging trend in European countries. These individuals are employed, radicalized, taught, trained and directed on different online platforms. In these cases, the threat comes from an individual, the 'lone wolf', living next door, being trained online, and organizing violence without being suspected of unlawful activity.[23] This phenomenon is not common in Pakistan yet, but the situation might aggravate in future if adequate timely counter measures are not taken.

For terrorist groups, un-attributable currency remains an ideal medium to transmit funds. New online activity shows increased interest of extremist/terrorist groups in Bitcoins or other crypto-currencies.[24] Crypto-currencies are classified as digital or virtual currencies which can be attained and spent without any intervention from the government and banks. For instance, one of Islamic State's associated online site, Akhbar al-Muslimin conducted a fundraising campaign using Bitcoin's platform in November 2017.[25] Middle Eastern Research Institution (MERI) also reported a terrorist telegram channel which ran a graphical campaign for donation of Bitcoin for Syrian fighters.[26] Another recent incident highlighted case of a New York based woman accused of sending Bitcoin to Islamic State.[27] In the last two years, Bitcoin has found space in Pakistan as well. In May 2017, it was reported that Federal Board of Revenue (FBR) investigated few cases of Bitcoin traders, probably to dodge taxes or launder money. Pakistani government has not recognized crypto-currency (Bitcoin) as legal tender but it has also not formulated any legal framework to prevent its use. Non-existence of relevant law might create space for use of crypto-currency for terrorist activities in the country in future.

Cyber-attacks are an established threat, linked to commercial as well as private spaces. The trends are disturbing which threaten governments, businesses, and the people in general. Global cyber viruses like WannaCry, Petya, NotPetya[28] and hacking of bank account through ATM in Pakistan[29] are examples of growing threat. There is no reported incident of cyber-attack from a terrorist organization yet in the country but the potential exists. There are some striking features of this medium that may attract its use by terrorists: first; it is cheaper than traditional methods, second; cyber-terrorism is more anonymous hence difficult to trace the perpetrators, third; variety and number of targets are enormous, fourth; it can be conducted remotely, and lastly, cyber-terrorism has the potential to directly affect a large number of people simultaneously.

Measures Against Virtual Terrorist Threat

The common misuse of internet in Pakistan is cybercrime but now, existence of terrorist groups and their ability to use cyberspace is becoming increasingly more threatening. Taking cognizance of this threat, Pakistani authorities have taken some steps to counter it. In 2007, government of Pakistan established National Response Centre for Cyber Crime (NR3C) under the Federal Investigation Authority (FIA). This highly technical crime unit is responsible for mitigation of cybercrimes. There are some legal measures taken to curb terrorism, can also be extended to online terrorism.

Code of Criminal Procedure (CrPC) 1898[30] is a basic legislative measure against criminal activities in the country. The Telegram Act 1885 only deals with the telephone tapping or recording etc. Pakistan Telecommunication (reorganization) Act 1996[31] limits the spread of false and fabricated information, obscene material and glorification of an offense. Despite some limitations,[32] it offers the legal ground for prohibition of blasphemy and 'anti-state content'.[33] In August 2016, Prevention of Electronic Crimes Act (PECA) was passed, which deals with threats, including cybercrime and terrorist activities in cyberspace.

Anti-Terrorism Act (ATA) 1997,[34] the legal framework to curtail terrorist activities, give a broad definition of 'terrorist act'.[35] According to ATA, terrorism means:-

- Use or threat of use of coercion against government, public, foreign governments or international organizations.
- Use of force with the resolve to spread religious, sectarian and ethnic causes.
- Action which causes death, injury or damage to public property or kidnapping, taking hostage for ransom and taking law into own hand.
- Provocation of violence on religious, ethnic and sectarian basis, firing on religious congregations and places, burning public property and extortion of money.

- Interference with the communication system and preaching the beliefs and ideas through the means of communication against the will of government.
- Serious offence against public servant, police force and law enforcement officials.
- Any action done to the advantage of a proscribed organization.

In August 2016, Prevention of Electronic Crimes Act (PECA)[36] was promulgated. It has 27 clauses related to online criminal activities such as unauthorized access and copying of information system and critical infrastructure data, electronic forgery, electronic fraud, unauthorized use of identity information, unauthorized issuance of subscriber identity module (SIM) cards, unauthorized interception, child pornography, tampering of communication equipment, offence against dignity of a person, cyber stalking, spoofing, spamming etc. In addition to these, the bill has four clauses (glorification of an offence,[37] hate speech,[38] cyber terrorism,[39] and recruitment, funding and planning of terrorism[40]) which indirectly deal with the threat of online radical and terrorist activities.

Pakistan does not yet have a dedicated agency which particularly deals with the threat of terrorism in cyberspace. But there are some stakeholders dealing with terrorism on grounds such as civilian and military law enforcement agencies, FIA, Pakistan Telecommunication Authority (PTA), and National Counter Terrorism Authority (NACTA) and proposed Joint Intelligence Directorate (JID) etc. Role of these organizations extends to counter terrorism on the internet to some extent. Ministry of Interior has authorized its Counter Terrorism Wing (CTW)[41] to register cases under the Protection of Pakistan Act, Anti-Terrorism Act, anti-money laundering laws and cyber-crime laws.[42] According to cyber security expert Khawaja Muhammad Ali,[43] CTW is also working on a project 'Cyber Patrolling'. Under this project, CTW will identify individuals involved in criminal and terrorist activities online. After the implementation of PECA, Federal Cabinet approved FIA and Inter-Services Intelligence as the designated agency to deal with cyber crimes under PECA.

National Counter Terrorism Authority (NACTA)[44] is a significant pillar in the fight against terrorism. The agency is accountable for developing counter terrorism strategy and preparing short, medium and long term plans. It is, however, not yet fully operational. In 2015, Senate was informed that NACTA did not have sufficient staff for more than six years[45] and situation had not improved even after another year.[46] Current Interior Minister of Pakistan Mr. Ahsan Iqbal has acknowledged that NACTA could not play its effective role to implement National Action Plan.[47] On the other hand, during an interview, former interior minister Ch. Nisar Ali stated that NACTA was much more proactive and coordinated thousands of intelligence source reports.[48] He also mentioned that much delayed Joint Intelligence Directorate (JID) will be operational very soon. While talking in a conference in Islamabad, Mr. Ihsan Ghani,[49] National Coordinator of NACTA, informed that the agency has formulated its first-ever National Counter Extremism Policy Guidelines in October 2017. He also mentioned that a draft of national narrative is also being devised by NACTA with the consultation of different government organizations like FIA, IB, and individual experts on the subject, and representatives of provincial governments.

NACTA has developed and introduced a smart app named 'Tat'heer Drive'. This counter extremism and terrorism drive takes account of terrorist content both offline and online. A specialized 'National Cyber Counter Terrorism Unit' (NCCU) has been set up which has specific capabilities like technological cyber-security analysis etc. This unit is also authorized to build advanced software, for internet protocol capacity which can identify extremist and terrorist content, report and start a counter narrative. NACTA also began another 'Surfsafe Portal'.[50] It is an online reporting portal for

Pakistanis to report extremist online-content freely, securely and anonymously. While answering a question, Mr. Ihsan Ghani, the National Coordinator of NACTA,stated that another project 'Hate-speech App' is going to be launched in February 2018, which not only deals with the issues of hate-speech on ground but it will also help to counter online hate-speech. He also informed that NACTA was directing public-engagement programs promoting the theme "countering is better than blocking".

Under the provisions of PECA, PTA has also some powers to deal with the costumer communication. In addition, Lahore High Court has directed the federal government to amend PECA, to authorize PTA for blocking social media websites and information systems if blasphemous content is posted on them.[51] Apart from the civilian agencies, government has received a plan prepared by the ISI to let its operatives take anticipatory actions against entities, groups and organizations violating national security under PECA 2016.[52]

Some Suggested Initiatives

Although Pakistan is on the right track in its counter-terrorism efforts in cyber domain, there is a need for a more comprehensive approach towards solving this problem. To counter online terrorist threat, more academic research needs to be conducted to better comprehend the methods and motives behind terrorist use of internet. This under-researched area has vast prospects for improved academic exposure. Analysis of methods used by the terrorist groups on social media, identification of critical key structure which may be vulnerable to cyber-attacks and possible measures against potential threat to them, and internet's impact on population by extremists/radicals are a few research areas which could lead to a better understanding of the relationship between terrorism and internet. Government needs an explicit "Internet Monitoring Policy against Terrorist Use" with the resolve to deal with terrorist threat in cyberspace. There is a dire need to formulate laws specific to terrorism in cyberspace apart from existing legislative frameworks. Government also needs to regulate the issue of cryptocurrency to deal with the potential threat. Government needs to make an effort to offer awareness programs for youth, especially, on countering extremism, violence and terrorism in online spaces and exercising responsibility on the internet. Government, with the collaboration of civil society can lead the initiatives like 'Counter-Radicalization/Terrorism Hotlines and Centers', which can be approached by families of concerned individuals for offering immediate intervention to individuals under the course of being radicalized by online content.

During an interview, Mr. Amir Rana,[53] Director Pakistan Institute for Peace, puts this in another way, saying that, the government need to introduce 'Internet / Social Media Code of Ethics' which can be circulated through different campaigns, adding that the task is challenging but not impossible. NACTA is conducting some public engagement programs such as Tat'heer Drive, Surfsafe Portal and Hate-speech App to counter online extremist and terrorist content, but if there is lack of collaboration between NACTA and a common person then how is the authority going to the check response to such programs? There is a dire need for NACTA to come up with the idea of public inauguration of public-engagement programs involving students from different universities, research institutes and civil society. State electronic and print media can also be utilized to spread the message to the masses. There is immediate need for a national level organization on cyberspace like Computer Emergency Response Team (CERT) which will be responsible to act in any emergency situation to secure online critical infrastructure. As Pakistan has huge bulk of young people, there is a need to realize such huge number of population as skilled human resource in domain of cyber security. Pakistan can also develop "Internet Monitoring Labs" and connect these with different relevant departments like Police, Armed Forces and civilian and military Intelligence Agencies. These labs can assist the tasks particularly related to terrorism activities on the internet. Apart from these, Pakistan's armed forces need to come up with the idea of 'Cyber Command' to protect the defense-related critical infrastructure. Government needs to devote financial efforts in research and development (R&D) projects and advance smart apps which can help to detect apprehensive users or suspicious words to reach the perpetrators. Different technical institutions can be tasked the responsibility to help their student to develop Artificial Intelligence (AI) tools and smart apps for national level projects.

Government also needs to work on some formal and informal arrangements of cooperation with different states and international organizations for countering online terrorism. Such cooperative measures make condition for arrest and deportation, mutual legal support, relocating the criminal proceedings and sharing of evidence, mutual enforcement of rulings, freezing and conversion of assets and exchange of information between Law Enforcement Agencies (LEAs). Currently, the major threat is coming from social media apps around the world as terrorist groups are using Facebook and Twitter extensively. Pakistan can extend collaborative efforts with international IT companies like Google, Microsoft, Facebook, Twitter etc. These companies can help Pakistan in not only elimination of terrorist content but also it can also help Pakistan's law enforcement agencies to reach the actual perpetrators on the internet. Shanghai Cooperation Organization (SCO) is another platform which can be used to cooperate on international level as Pakistan is now member of the forum and the organization has terrorism and cyber security in its top agendas. Pakistan can use the tool of social media analytics to counter terrorist activities as social media is the online platform which is wildly used by the lone wolves and terrorist organizations for psychological warfare and propaganda.

Conclusion

The phenomenon of global terrorism has persisted as the most significant threat to states, international organizations and even a common man on the street for more than twenty years now. Institute for Economics and Peace reported in its Global Terrorism Index (GTI) 2017 that the total impact of terrorism on international economies is US$ 84 billion in 2016 and Pakistan remained one of five countries which got highest bearing of terrorism in last year.[54] While assessing the impact of use of internet by terrorist organizations, it can be stated that the online presence of terrorists is common in the prevalent situation all over the world. Brookings Institute published a research on 'ISIS propaganda on Twitter'. The study examined the encompassing use of twitter by ISIS operatives which puts out 18 media publications or statements every day. It also testified that ISIS has about 90,000 'dedicated twitter handlers' which abetted in enlisting 20,000 supporters.[55]

Despite all the sufferings and losses during war on terror, there are some issues which still need serious consideration and political will from Pakistani authorities. Government of Pakistan needs to differentiate the terms crime and terrorism clearly while regulating any of the conventional criminal or terrorist activity so that implementation and execution process does not contain any misperception on the part of law enforcement agencies. For instance, while one critically analyzes the definition of terrorism adopted by PECA which is extended from Anti-Terrorism Act, few features make it broad and bit ambiguous like hijacking, kidnapping, ransom and taking law into own hand and damage to property (burning vehicles). As these acts are abhorrent, they could be considered as criminal rather than terrorist acts in isolation. Talking about the definitional aspects of 'terror act', Mr. Amir Rana deliberated that current definition of terrorism which is also applicable on cyberspace, has delicate problems in it. The authorities need to narrow down the criteria and redefine it. While defining such a vital term, it must be kept in mind that motives must be defined rather than specifications, which makes the process of execution weak and distorted.

After acknowledging any risk to the national security, the most important step for states is to formulate a policy which gives guidelines to meet the objectives (in a particular realm) to mitigate the threat. As the presence of terrorist in online spaces is securitized in South Asia, specifically in Pakistan, the issue needs a policy directive to address the prevailing threat. Unfortunately, Pakistan could not meet the requirement yet by framing Cyber Security Policy but Pakistan has formulated it first ever 'Digital Pakistan Policy' in 2017, acknowledging the fact that the country needs a roadmap to go ahead in IT sector. Coming to the issue of legal measures, it is foremost challenge for the countries to define legal regime to handle a particular issue. Pakistan is not as mature in legislation as the Western democracies, but the country is taking countermeasures to stop terrorism within the state. Major criticism on Pakistan's legal framework is that, Pakistan is practicing most of the laws as 'British Legacy' and did not bring new laws with the changing threat environment such as Telegram Act (1885) and Code of Criminal Procedure (1898) are still being implemented just with some amendments. Pakistan has regulated anti-terrorism laws in offline as well as online spaces such as Pakistan Telecommunication Act (1996), Anti-Terrorist Act (1997), Electronic Transaction Ordinance (2002), Investigation of Fair Trial Act (2013), and Prevention of Electronic Crimes Act (2016) but all these measures are not sufficient to counter terrorism in cyberspace. Legal counter terror frameworks can never, separately, deal with the issues without active and prominent executive bodies. Unfortunately, the sub-continent has been unlucky since long for not having and maintaining vigorous executive bodies (free of corruption) to run the matters of government. Inactive and corrupt government institutions in Pakistan have always overturned the performance of different sectors, which also impacts the countering of terrorism in the cyber domain.

Coming to counter terrorism efforts, Pakistan has realized the need of the hour and has done incredible hard work both in legal and executive domains, but when the issue of terrorism in cyberspace comes; the country lags far behind the developed countries. As military and intelligence community of any state are the most important part of counter terror strategy, the states need some other significant institutions in civilian domain that can work well alongside with military. Pakistan is employing available means to counter the threat as counter terrorism authorities such as FIA, NACTA, civil and military intelligence services are working hard to accomplish the combined objective. But lack of cooperation between all the stakeholders is still a major problem, an inactive Joint Intelligence Directorate is just one example of it. The task ahead for Pakistan will be better coordination of all the agencies involved in countering terrorism in general, and cyberterrorism in particular. Moreover, there is a need to re-double efforts in improving counterterrorism legal frameworks and executive measures. Pakistan also needs to organize its best efforts to collaborate with regional and international forums and countries; and global IT companies to counter online terror threat.

Afeera Firdous is a
Research Assistant at CISS

Endnotes:

[1] "Foreign Terrorist Organization," US Department of the State, https://www.state.gov/j/ct/rls/other/des/123085.htm

[2] Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Washington D.C.: Woodrow Willson Centre Press, 2015), 6.

[3] The term first devised by William Gibson in his science fiction novel 'Neuromancer' in 1984.

[4] US Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: US Government Printing Office, February 2017), 60.

[5] B. Hoffman, *Inside Terrorism* (New York: Oxford University Press, 2006), 3.

[6] P. R. Viotti and M. V. Kauppi, *International Relations and World Politics* (New York: Pearson, 2013), 254.

[7] United Nations, "UN Global Counter Terrorism Strategy," https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy

[8] NATO Cooperative Cyber Defense Centre of Excellence, "International Code of Conduct for International Security," https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

[9] Reuter Staff, "Factbox: How UK's anti-terrorism internet unit works," *Reuters,* October 4, 2010, https://www.reuters.com/article/us-security-internet-factbox/factbox-how-uks-anti-terrorism-internet-unit-works-idUSTRE6932AY20101004

[10] Alissa J. Rubin, "Lawmakers in France move to vastly expand surveillance," *New York Times*, May 5, 2015, https://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html?_r=0

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

[12] Rob Price, "Google, Facebook, Microsoft and Twitter are Working Together to Tackle Terrorist Propaganda," *Business-Insider,* December 06, 2016, http://www.businessinsider.com/r-web-giants-to-cooperate-on-removal-of-extremist-content-2016-12

[13] "Internet Users in Pakistan," Internet Live Stats, http://www.internetlivestats.com/internet-users/pakistan/

[14] Simon Kemp, "Digital, social and mobile APAC in 2015," Pakistan Advertisers Society, https://www.pas.org.pk/digital-social-mobile-in-apac-in-2015/

[15] Jahanzaib Haque and Omar Bashir, "Banned Outfits in Pakistan operate openly on Facebook" *Dawn,* updated September 14, 2017, https://www.dawn.com/news/1335561

[16] M. Hussain Khan and Imran Gondal, "Woman held after encounter in Lahore went to Syria for training," *Dawn,* April 17, 2017, https://www.dawn.com/news/1327453

[17] Staff Report, "Female MBBS student with 'extremists' views goes missing," *SAMAA,* March 16, 2017, https://www.samaa.tv/pakistan/2017/03/female-mbbs-student-with-extremist-views-goes-missing/

[18] Staff Report, "Noreen Laghari says she was going to be used as suicide bomber," *SAMAA,* April 17, 2017, https://www.samaa.tv/pakistan/2017/04/noreen-laghari-says-she-was-going-to-be-used-as-suicide-bomber/

[19] Ansar-ul-Sharia, a splinter group of Islamic State, formed in April 2017 with a first claimed attack in Karachi.

[20] Staff Report, "Ansarul Sharia group is limited to Karachi, says DG Rangers," *The Express Tribune,* September 10, 2017, https://tribune.com.pk/story/1502356/ansarul-sharia-limited-karachi-rangers-dg/

[21] Zeeshan Shah, "Ansar-ul-Shariah members used code words to communicate internally," *Geo News,* September 9, 2017, https://www.geo.tv/latest/157348-ansar-ul-shariah-members-used-codewords-to-communicate-internally

[22] Ali Leghari, "Terrorist group Ansarul Sharia developed mobile apps for highly secure communication," *TechJuice,* September 9, 2017, https://www.techjuice.pk/ansarul-sharia-mobile-apps-secure-communication/

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

[24] Joe Barnes, "Bitcoin WARNING: ISIS using cryptocurrency to fund reign of terror as Bitcoin price soars," *Express*, December 17, 2017, https://www.express.co.uk/finance/city/893151/Bitcoin-price-latest-news-ISIS-terror-cryptocurrency.

[25] Leigh Cuen, "Terrorists are increasingly interested in Bitcoin," *IBTimes*, November 22, 2017, http://www.ibtimes.com/terrorists-are-increasingly-interested-bitcoin-2631713

[26] Ibed.

[27] Alexandra Ma, "A New York Woman accused of sending bicoins to ISIS could spend 90 years in prison," *Business Insider,* December 15, 2017, http://www.businessinsider.com/zoobiah-shahnaz-charged-after-sending-bitcoin-to-isis-from-long-island-2017-12

[28] Alex Hern, "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017," *The Guardian,* December 30, 2017, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

[29] Staff Report, "Hundreds of Pakistanis lose millions in major ATM skimming fraud," *Geo News,* December 4, 2017, https://www.geo.tv/latest/170648-hundreds-of-karachiites-lose-millions-in-major-atm-skimming-fraud

[30] Amended twice in 2013 and 2014.

[31] Federal Investigation Agency, 'Pakistan Telecommunication (Re-organization) Act 1996,' http://www.fia.gov.pk/law/Offences/23.pdf

[32] Ambiguous and unclear definitions leading to restriction on the freedom of expression.

[33] 'Pakistan Telecommunication (Re-organization) Act January 2012: Legal Analysis, Article 19," https://www.article19.org/data/files/medialibrary/2949/12-02-02-Pakistan.pdf

[34] "Anti-Terrorism Act 1997," http://www.ppra.org.pk/doc/anti-t-act.pdf

[35] Section 6 of ATA 1997.

[36] National Assembly, "Prevention of Electronic Crimes Act 2016," http://www.na.gov.pk/uploads/documents/1470910659_707.pdf

[37] Section 9 of PECA 2016.

[38] Section 11 of PECA 2016.

[39] Section 10 (a) and (c) of PECA 2016.

[40] Section 12 of PECA 2016.

[41] Counter Terrorism Wing is part of FIA since 2003. It deals with the arrest and prosecution of the Most Wanted Terrorist and became a center of excellence for specialized counter terrorist investigation.

[42] "FIA empowers to register cases of terrorism," *Dawn,* September 30, 2015, https://www.dawn.com/news/1209848

[43] Khawaja Muhammad Ali is Certified Information Systems Auditor (CISA)/ Certified in Risk and Information Systems Control (CIRSC). He is also Director and CSX Liaison of Information Systems Audit and Control Association (ISACA) Pakistan. Previously, he worked with the Ministry of IT, Government of Sindh as an Advisor.

[44] Agency was launched in 2008 but its mandate was finalized with the recognition of NACTA Act in 2013.

[45] Amir Wasim, "NACTA is functioning without formal staff, Senate told," *Dawn,* November 12, 2015, https://www.dawn.com/news/1219112

[46] "NACTA facing dearth of officers and resources, says coordinator," *Pakistan Today,* August 18, 2016, https://www.pakistantoday.com.pk/2016/08/18/nacta-facing-dearth-of-officers-resources-says-coordinator/

[47] Imran Mukhtar, "NACTA failed to effectively implement NAP: Ahsan," *The Nation,* August 23, 2017, http://nation.com.pk/national/23-Aug-2017/nacta-failed-to-effectively-implement-nap-ahsan

[48] Geo News, "Program Jirga," broadcasted on September 10, 2017, https://www.youtube.com/watch?v=oCyy76S86yI

[49] Mr. Ihsan Ghani joined NACTA as National Coordinator in 2015.

[50] National Counter Terrorism Authority, "Safe Surf Portal," http://nacta.gov.pk/httpssurfsafe-pk/

[51] Mahmood Idrees, "Govt told to empower PTA for blocking social media websites on not removing blasphemous material," *Daily Pakistan,* May 2, 2017, https://en.dailypakistan.com.pk/pakistan/govt-told-to-empower-pta-for-blocking-social-media-websites-on-not-removing-blasphemous-material/

[52] Zahid Gishkori, "Govt accepts ISI's role in checking cybercrimes," *The News*, October 20, 2016 https://www.thenews.com.pk/print/158580-Govt-accepts-ISIs-role-in-checking-cyber-crimes

[53] Muhammad Amir Rana is a security and political analyst and the director of Pak Institute for Peace Studies (PIPS), an independent Islamabad-based think tank.

[54] "Global Terrorism Index 2017," Institute for Economic and Peace, https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf

[55] Shruti Pandalai, "ISIS in Indian: Writing on the (Facebook) wall," *IDSA*, May 6, 2016, http://idsa.in/idsanews/isis-in-India-writing-on-the-facebook-wall_060516