ONLINE RADICALIZATION: BANGLADESH PERSPECTIVE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

MOHAMMAD ISTIAQUE RASHID, MAJOR, BANGLADESH ARMY
M.Sc., Bangladesh University of Professionals, Dhaka, Bangladesh, 2016

Fort Leavenworth, Kansas
2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
9-06-2017	Master's Thesis	AUG 2016 – JUN 2017

4. TITLE AND SUBTITLE

Online Radicalization: Bangladesh Perspective

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Mohammad Istiaque Rashid

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The internet has significantly increased terrorists' reach, and person to person contact is no more essential to radicalize people. Some terrorist organizations in Bangladesh are also maneuvering in the cyber domain to spread their ideologies and radicalize people. To prevent radicalization through cyberspace, Bangladesh mostly implements hard powers such as removing contents and restricting access to the internet. However, freedom of speech and access to information are prime requirements for a prosperous and democratic society. Therefore, Bangladesh should develop an effective strategy to counter radicalization without impinging citizens' freedom of speech. The country, nonetheless, faces challenges due to lack of coordination among the counter-terrorism agencies, and lack of positive initiatives to grow enduring social resilience against radicalization. Bangladesh may harness benefits by adopting key elements of seemingly successful programs of other countries. It should also create a strategy for appealing positive messaging to foster inter-faith respect and communal harmony where counter-narratives will be embedded. Besides, developing ethics and responsibility of the Internet users will create a self-monitoring system in the cyber domain. Finally, constructive measures will enable Bangladesh to develop a sustainable counter radicalization mechanism without impinging citizens' democratic rights.

15. SUBJECT TERMS

Bangladesh, cyber, online, social media, radicalization, FBI, NCTC, Indonesia, and Malaysia

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	107	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Mohammad I. Rashid

Thesis Title: Online Radicalization: Bangladesh Perspective

Approved by:

_____, Thesis Committee Chair
John G. Breen, Ph.D.

_____, Member
LTC Benjamin C. Croom, M.A.

_____, Member
Daniel C. Honken, M.S.

Accepted this 9th day of June 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

ONLINE RADICALIZATION: BANGLADESH PERSPECTIVE by Major Mohammad Istiaque Rashid, 107 pages.

The internet has significantly increased terrorists' reach, and person to person contact is no more essential to radicalize people. Some terrorist organizations in Bangladesh are also maneuvering in the cyber domain to spread their ideologies and radicalize people. To prevent radicalization through cyberspace, Bangladesh mostly implements hard powers such as removing contents and restricting access to the internet. However, freedom of speech and access to information are prime requirements for a prosperous and democratic society. Therefore, Bangladesh should develop an effective strategy to counter radicalization without impinging citizens' freedom of speech. The country, nonetheless, faces challenges due to lack of coordination among the counter-terrorism agencies, and lack of positive initiatives to grow enduring social resilience against radicalization. Bangladesh may harness benefits by adopting key elements of seemingly successful programs of other countries. It should also create a strategy for appealing positive messaging to foster inter-faith respect and communal harmony where counter-narratives will be embedded. Besides, developing ethics and responsibility of the Internet users will create a self-monitoring system in the cyber domain. Finally, constructive measures will enable Bangladesh to develop a sustainable counter radicalization mechanism without impinging citizens' democratic rights.

ACKNOWLEDGMENTS

At first, I would like to convey my deepest gratitude to my committee – Dr. John G. Breen, Lieutenant Colonel Benjamin C. Croom, and Mr. Daniel C. Honken – for assisting and guiding me throughout the process. It would be impossible for me to finish this research without their mentorship and valuable inputs. My committee members' recommendations and additional hours of assistance were the keys throughout, and I am immensely grateful to them.

Besides, special thanks to my wife and son for remaining as a constant source of inspiration. Finally, all praise to the Almighty for giving me the patience and strength to complete this research.

TABLE OF CONTENTS

Page

ACRONYMS

ABT	Ansarullah Bangla Team
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CREX	Community Resilience Exercise
DGFI	Directorate General of Forces Intelligence
FBI	Federal Bureau of Investigation
ICT	Information and Communication Technology
IC3	The Internet Crime Complaint Center
IMPACT	International Multilateral Partnership against Cyber Threats
ISIL	Islamic State of Iraq and the Levant
LEA	Law Enforcing Agency
NCC	National Cybersecurity Council
NCTC	National Counter Terrorism Center
NSI	National Security Intelligence
NTMC	National Telecommunication Monitoring Centre
NYPD	New York Police Department
RAB	Rapid Action Battalion
SB	Special Branch

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

Background

On July 1, 2016, six Islamist militants from Bangladesh attacked Holey Artisan Bakery, an upscale restaurant in the Dhaka diplomatic zone that became a lead story in the world media. The Government of Bangladesh claims the militants to be home-grown terrorists.[1] However, the instantly released pictures of dead bodies on the Islamic State of Iraq and the Levant (ISIL) website suggest that the terrorist group was able to maintain a virtual connection with the ISIL during the time of the attack.[2] After a 12-hour siege, Bangladeshi security forces conducted a rescue operation at the restaurant in the early hours of July 2, 2016, and freed 13 hostages.[3] Unfortunately, the terrorists killed 20 hostages, including Italian, Japanese, Indian, and the U.S. citizens. Four militants and two police officers were killed during the incident, and one militant was arrested. This attack was reportedly the 24th terrorist attack in Bangladesh since 2015, and the deadliest of

[1] Julfikar Ali Manik and Geeta Anand, "After Slaughter, Bangladesh Reels at Revelations About Attackers," *The New York Times*, July 3, 2016, accessed March 14, 2017, https://www.nytimes.com/2016/07/04/world/asia/bangladesh-dhaka-terrorism.html.

[2] Chris Summers, "Pictured: The Grinning ISIS Terrorists who Hacked 20 Innocent Victims Including Westerners to Death but Spared those who could Recite the Koran in Bangladesh Attack," *The Daily Mail*, July 2, 2016, accessed March 14, 2017, http://www.dailymail.co.uk/news/article-3671586/Pictured-grinning-ISIS-terrorists-hacked-20-innocent-victims-including-westerners-death-spared-recite-Koran-Bangladesh-attack.html.

[3] Andrew Marszal and Chris Graham, "20 Hostages Killed in 'ISIL' Attack on Dhaka Restaurant Popular with Foreigners," *The Telegraph*, July 2, 2016, accessed November 14, 2016, http://www.telegraph.co.uk/news/2016/07/01/gunmen-attack-restaurant-in-diplomatic-quarter-of-bangladeshi-ca/.

all.[4] Surprisingly, the attackers were not so called traditional "Mullah"; they were upper-class youths who were students in good universities at home and abroad. Their friends mentioned them as fun-loving and energetic juveniles. However, after the incident, a few of their friends informed the investigating authorities that they observed a few unusual and apparently radical changes in their behaviors. Likewise, there may be thousands of other youths in the country who are covertly in the process of radicalization. Conventional wisdom appears to suggest a source of this radicalization is religious in nature. A survey conducted by Bangladesh Enterprise Institute, a leading research center in Bangladesh, reveals that the recent trend of radicalization in Bangladesh is mostly associated with Islamist radicalization.[5] Therefore, questions arise, why and how the upper-class youths, who were never educated in traditional madrasas, are being radicalized. Many analysts suggest that Islamic radicalization has escalated to a new level in Bangladesh, likely due to the spread of the internet.[6]

The U.S. Department of Justice defines "online radicalization" as a process of introducing an individual to an ideological message or beliefs through the internet that

[4] The Indian Express, "List of Recent Attacks in Bangladesh Blamed on Radical Islamists," July 2, 2016, accessed November 14, 2016, http://indianexpress.com/article/world/world-news/list-of-recent-attacks-in-bangladesh-blamed-on-radical-islamists-2888881/.

[5] Farooq Sobhan, *The Role of Education in Countering Radicalization in Bangladesh* (Dhaka: Bangladesh Enterprise Institute, 2015), VII.

[6] Tanbir Uddin Arman, "New Media, Digital Radicalization and Social Security," *The Bangladesh Today*, September 8, 2015, accessed November 14, 2016, http://thebangladeshtoday.com/2015/09/new-media-digital-radicalization-and-social-security/.

encourages adopting extreme views and terrorist acts.[7] It is a fluid and highly individualized process, and a number of socio-cultural factors may contribute to this. Globalization and its resultant revolution in communication technologies seem to expedite this process by providing social networking tools such as Facebook, Twitter, YouTube, Blogs, MySpace, and Google+. These social media outlets seem effective to radicalize people by spreading violent ideologies and recruit members.[8] The internet has become the easiest way to reach any audience, and person to person contact is no longer essential to radicalize people. The UK newspaper, *The Guardian*, termed the internet as the "biggest breeding ground for violent extremism."[9] Norwegian terrorist Anders Behring Breivik admitted that he was radicalized in cyberspace, and committed the massacre to defend Norway from multiculturalism.[10] Thus, the internet facilitates the radicalization, and religious or cultural misinterpretations often trigger the process.

Terrorists adopt different techniques to spread their messages through the internet. For instance, to avoid interception, extremists draft an email message and save it as a draft instead of sending it. Anyone with access to that email account can log in and read

---

[7] Community Oriented Policing Service, "Online Radicalization to Violent Extremism" (Awareness Brief, U.S. Department of Justice, Washington, DC, 2014), 1.

[8] Maeghin Alarid, *Impunity: Countering Illicit Power in War and Transition*, edited by Michelle Hughes and Michael Miklaucic (Washington, DC: National Defense University, 2012), 365.

[9] Alan Travis, "Internet Biggest Breeding Ground for Violent Extremism," *The Guardian*, February 5, 2012, accessed December 17, 2016, https://www.theguardian.com/uk/2012/feb/06/internet-violent-extremism-breeding-ground.

[10] Matthew Price, "Anders Breivik describes Norway Island Massacre," *BBC*, April 20, 2012, accessed November 11, 2016, http://www.bbc.com/news/world-europe-17789206.

the message. This technique is known as a "dead drop," and is less subject to interception than an email that has been sent. They also post training manuals online or even hack a legitimate website to hide training materials "deep in seemingly innocuous subdirectories of the legitimate site," a process known as "parasiting."[11] "Narrowcasting" is another way where terrorists keenly observe and exploit the social networking sites. According to Gabriel Weimann, "Narrowcasting aims messages at specific segments of the public defined by values, preferences, demographic attributes, or subscription."[12] Terrorists tailor various online pages like blogs and name chat rooms in an appealing manner that match the profile of a particular social group they intend to target. These different techniques suggest that extremist groups are innovating ways to exploit the internet and reach their target audiences.

Of particular note, social networking sites have numerous advantages that the terrorists may exploit to spread their values. Since these are dynamic platforms for content sharing, it is extremely difficult to control or impose restrictions on social websites, whereas static websites are more susceptible to government interception. Hence, terrorist groups seem to exploit the relative advantages of social media. It provides easy access to the well-educated cyber-savvy youths as well. A sophisticated computer with a network connection is no longer essential to share, upload or download files and videos on these social networking sites. Anyone can gain access to this content

[11] Technical Analysis Group, "Examining the Cyber Capabilities of Islamic Terrorist Groups" (Research, Dartmouth College, New Hampshire, 2003), accessed January 21, 2017, www.ists.dartmouth.edu/library/164.pdf.

[12] Gabriel Weimann, *New Terrorism and New Media* (Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014).

using a smartphone from any location.[13] Therefore, the social networking sites seem to increase the reach of the extremists.

Furthermore, certain features of social media appear to increase the chances of cyber-enabled engagement and radicalization. Terrorists usually create different secret or closed groups on the social networking sites with appealing names and add their targeted audiences. It blurs the geographic limitations by engaging like-minded people in the same group. It also enables conveying specific messages to the target audiences to influence their behaviors and emotions. They discuss various controversial issues in these groups and appeal to the human sentiment. Moreover, they can engage a large number of people simultaneously through these groups and blogs. Social media posts may also affect the public opinion on a large scale and can be used to create sympathizers.

In the context of Bangladesh, Information and Communication Technology (ICT) development is likely an imperative for the country's economic prosperity, but it may also increase the probability of online radicalization. The Government of Bangladesh has given top priority to the development of ICT and digitization of different sectors. The number of internet users has almost doubled in the last four years. Bangladesh was ranked 124th in the 2016 United Nations E-Government Survey among the 193 countries advancing by 24 steps.[14] In 2014 and 2012, Bangladesh was ranked 148 and 150 respectively. Table 1 shows the rise of internet users in Bangladesh since year 2010:

---

[13] Weimann, *New Terrorism and New Media*, 3-4.

[14] United Nations Department of Economic and Social Affairs, "UN E-government Knowledge Database," accessed January 21, 2017, https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/14-Bangladesh.

Table 1. Internet Users in Bangladesh

Year	Internet Users	Penetration (% of Pop)	Total Population	1Y User Change	Population Change
2016	21,439,070	13.2 %	162,910,864	10.4 %	1.19 %
2015	19,420,674	12.1 %	160,995,642	27.2 %	1.21 %
2014	15,271,441	9.6 %	159,077,513	46.6 %	1.22 %
2013	10,419,535	6.6 %	157,157,394	34.2 %	1.22 %
2012	7,762,869	5 %	155,257,387	12.5 %	1.21 %
2011	6,903,253	4.5 %	153,405,612	23.1 %	1.18 %
2010	5,609,821	3.7 %	151,616,777	20.7 %	1.14 %

Source: Internet Live Stats, "Bangladesh Internet Users," accessed November 15, 2016, http://www.internetlivestats.com/internet-users/bangladesh/.

According to Farooq Sobhan, a security expert and the president of Bangladesh Enterprise Institute, extremist groups are using online platforms, especially social networking sites, to spread their messages and create rifts among people.[15] It appears that extremists also select and recruit members, collect funds, and maintain contact with them through various online programs. They create different blogs with their messages and continuously monitor those to understand social perceptions. These extremist groups are seemingly exploiting popular online platforms like social media, video and content sharing sites, and online games to mislead people. Extremists in Bangladesh attempt to

[15] Sobhan, *The Role of Education in Countering Radicalization in Bangladesh*, VII-VIII.

spread "hate speech" through these communication tools to create rifts among various religions, and destabilize communal harmony. Their hate speeches and repulsive posts spread rapidly in Bangladesh where peoples' ethnoreligious sentiment is very high.[16] Hate speeches may have already triggered communal violence in the country, for example, the torching and vandalizing of Hindu temples on October 30, 2016.[17] It appears that extremists deliberately post and tag offensive materials on various social media sites to mobilize people to carry out attacks on religious and ethnic minority groups.

Some Islamic extremist groups in Bangladesh have developed cyber-related technological capabilities. Iftekharul Bashar, a security analyst in Bangladesh, terms the recent online radicalization in Bangladesh as the "second wave of radicalization."[18] The first wave started during 1999-2005 and resulted in a number of violent incidents in the country. As a consequence of the government action against extremist and terrorist organizations, that wave faded away.[19] However, this second wave of radicalization seems to be different. The recent wave appears to depend on new technologies and spreading of messages through cyberspace. Today, domestic Islamist extremist groups

[16] Ibid., 10.

[17] Julfikar A. Manik and Ellen Barry, "Hindu Temples and Homes in Bangladesh Are Attacked by Muslim Crowds," *The New York Times*, November 2, 2016, accessed March 4, 2017, https://www.nytimes.com/2016/11/03/world/asia/hindu-muslim-bangladesh.html.

[18] Iftekharul Bashar, "Violent Radicalisation in Bangladesh: A Second Wave?," *The Nation*, 2013, accessed December 18, 2017, http://www.nationmultimedia.com/news/opinion/aec/30217330.

[19] Ibid.

like Hijb ut Tahrir, Al Qaeda in the Indian Subcontinent, as well as pro-ISIL supporters are believed to use the internet as one of the main ways to spread propaganda and recruit new members.[20] One group that demands special attention is the newly formed Ansarullah Bangla Team (ABT). It has a large group of followers who are mostly from private universities. They have a strong presence in social networking sites and have the expertise to spread propaganda through cyberspace.[21] The educated youths harness resources from different websites of global terrorist groups and translate them into the local language.[22]

The youths of Bangladesh are particularly vulnerable to online radicalization. As per the Population Reference Bureau in 2016, Bangladesh had a total of 46.7 million youths - ages between 10 to 24 years - that is approximately 30% of the total population.[23] A large number of youths are tech-savvy and addicted to social media. For example, a research conducted on the youths residing in Dhaka City reveals that almost half of them spend long hours on the social media sites and believe it to be an important

[20] Shahab E. Khan, "Bangladesh: The Changing Dynamics of Violent Extremism and the Response of the State," *Small Wars and Insurgencies* 28, no. 1 (2017): 192-193.

[21] Terrorism Research and Analysis Consortium, "Ansarullah Bangla Team (ABT)," accessed March 4, 2017, https://www.trackingterrorism.org/group/ansarullah-bangla-team-abt.

[22] Global Security, "Ansarullah Bangla Team (ABT)," accesses March 4, 2017, http://www.globalsecurity.org/military/world/para/abt.htm.

[23] Population Reference Bureau, "Bangladesh," accessed November 10, 2016, http://www.prb.org/DataFinder/Geography/Data.aspx?loc=378.

part of their lives.[24] Sobhan claims that a majority of the youths are not aware of online radicalization due to a lack of any organized awareness program by the government or academic institutions.[25] This unawareness provides a window of opportunity for the terrorists to reach them without any personal contact. The young people are often driven by their emotions, and without validating a message, they may act abruptly.[26] The incidents of communal violence demonstrate the effects of false messages on the youths. Moreover, recruiting the educated youths may be more valuable to the extremist groups than an ordinary recruitment. Tariq Karim and Dr. Madhumita Srivastava Balaji, security experts in the Indian sub-continent, agree that youths with technological knowledge can reinforce the terrorists' ability in the cyber domain.[27] They can create different virtual links to maintain contact with global extremist groups while deceiving government restrictions. They may also produce greater effects in the upper-class society in the country.[28] As a result, the extremist groups of Bangladesh attempt to exploit the juvenile emotion and extend their recruitment efforts through cyberspace.

---

[24] S. M. Al-Jubayer, "Use of Social Networking Sites Among the Teenagers; A Study of Facebook Use in Dhaka City," *Journal of International Social Issues* 2, no. 1 (March 2013): 37.

[25] Sobhan, *The Role of Education in Countering Radicalization in Bangladesh,* 10-11.

[26] Ibid.

[27] Tariq Karim and Dr. Madhumita S. Balaji, *Rising Trend of Religious Radicalization in Bangladesh* (New Delhi: Vivekananda International Foundation), 7-8.

[28] Sobhan, *The Role of Education in Countering Radicalization in Bangladesh*, 10.

In an attempt to counter these extremists' efforts, the Government of Bangladesh mainly implements coercive measures. Most of the measures aim to either remove content or restrict access to the internet. For example, the Government of Bangladesh blocked Facebook and YouTube on November 18, 2015, due to the posting of some anti-religious and violent content. It was, however, reopened after 21 days.[29] This temporary blockade appeared ineffective since many people bypassed the online restrictions by using proxy servers. Internet users are likely to find some alternative means to evade government restrictions if imposed in the future. Therefore, forcible methods appear to be less effective tools to defeat radical ideas.

Sobhan notes that Bangladesh might not have properly appreciated the potentials of the internet to spread violent ideologies, radicalize and recruit people, and its adverse effects on national security.[30] The United States Institute of Peace defines countering violent extremism and radicalization as "the realm of policy, programs, and interventions designed to prevent individuals from engaging in violence associated with radical political, social, cultural, and religious ideologies and groups."[31] In an attempt to prevent radicalization through cyberspace, at times the government of Bangladesh impinges citizens' freedom of expression and access to information. However, infringement on

---

[29] Sneha Shankar, "Bangladesh Unblocks Facebook After 21 Days; WhatsApp, Viber Restrictions Stay," *International Business Times*, October 12, 2015, accessed November 14, 2016, http://www.ibtimes.com/bangladesh-unblocks-facebook-after-21-days-whatsapp-viber-restrictions-stay-2219519.

[30] Sobhan, *The Role of Education in Countering Radicalization in Bangladesh*, 1-2.

[31] Georgia Holmer, *Countering Violent Extremism: A Peacebuilding Perspective*, Special Report 336 (Washington, DC: United States Institute of Peace, 2013), 2.

citizens' democratic rights and shielding them from information may impede socio-economic progress. Therefore, it is challenging to make a balance between two competing requirements: preventing online radicalization and ensuring a free flow of information. With this information, the coercive measures of the Government of Bangladesh seem neither practical nor desirable. In this context, Bangladesh should seriously assess the effectiveness of her programs to prevent radicalization through cyberspace without impinging citizens' freedom of speech and access to valuable information.

This chapter introduces the background and the problem of online radicalization in Bangladesh. The researcher has introduced the primary and secondary research questions in this chapter that will guide subsequent chapters and findings. This study emphasizes the understanding of online radicalization from a Bangladeshi perspective. It is a serious security concern for Bangladesh if the challenges remain unaddressed. This study may help the Government of Bangladesh, the military, and scholars to understand the current weaknesses of countering online radicalization. After identifying the voids, this research will suggest an integrated mechanism against online radicalization to the Government of Bangladesh.

Research Question

The purpose of this study is to evaluate the strategy of Bangladesh to counter online radicalization. The research questions are:

Primary Question

Are the counter-terrorism efforts of Bangladesh effective to prevent online radicalization without impinging the citizen's access to information?

Subsidiary Questions

1. What is the current strategy of Bangladesh to counter online radicalization?
2. What are the significant aspects of successful models of different countries to prevent online radicalization?
3. How can Bangladesh develop an effective mechanism to prevent radicalization through the cyberspace without shielding its citizens from information?

Assumptions

The key assumption of this study is that terrorist organizations will continue to use the internet as a successful means of radicalization. They will attempt to radicalize and recruit people, foment communal violence, and spread propaganda by using the internet. Terrorist organizations will continue to present a threat to the security of Bangladesh. Another assumption is that Bangladesh will remain as a democratic country with stable governance system in the foreseeable future.

Definitions of Terms

"Counter-radicalization seeks to prevent non-radicalized populations from being radicalized. The objective is to create individual and communal resilience against

cognitive and violent radicalization through a variety of non-coercive means."[32] The U.S. government uses the term "Countering Violent Extremism" (CVE) to describe its foreign and domestic counter-radicalization efforts.

"Cybersecurity means all organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken against crime, attack, sabotage, espionage, accidents, and failures."[33]

"Cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address) on those networks, and the system data (such as routing tables) that support them."[34] The U.S. Military Joint Publication 3-12 describes three layers of cyberspace: physical network, logical network, and cyber-persona. The physical network includes the geographic components and the physical network components where the data travel. The logical network consists of those elements that are interrelated to one another in a way that is abstracted from the physical network. The cyber-persona is a further abstraction of the logical network. The cyber-persona layer consists of the people actually on the network.[35]

---

[32] Peter R. Neumann, "Countering Online Radicalization in America" (Homeland Security Project Report, Bipartisan Policy Center, Washington, DC, December 2012), 13.

[33] The Vice Chairman of the Joint Chiefs of Staff, *Cyberspace Operations Lexicon* (Washington, DC: The Government Printing Press), 7.

[34] Office of the Joint Staff, Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington, DC: Government Printing Office, 2013), V.

[35] Ibid.

The Internet, a subset of cyberspace, is a system of interconnected computer networks. It comprises both hardware and software that facilitate data transfer across a network. It functions primarily as a data-exchange system and carries a broad range of resources.

"Online radicalization to violence is the process by which an individual is introduced to an ideological message and belief system that encourages movement from mainstream beliefs toward extreme views, primarily through the use of online media, including social networks such as Facebook, Twitter, and YouTube."[36]

"Radicalization is a personal process in which individuals adopt extreme political, social, and or religious ideals and aspirations, and where the attainment of particular goals justifies the use of indiscriminate violence. It is both a mental and emotional process that prepares and motivates an individual to pursue violent behavior."[37]

Social media are computer-mediated technologies that facilitate the creation and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks. The variety of stand-alone and built-in social media services currently available introduces challenges of definition; however, there are some common features:

1. Social media are interactive Web 2.0 Internet-based applications.

---

[36] Community Oriented Policing Service, "Online Radicalization to Violent Extremism" (Awareness Brief, U.S. Department of Justice, Washington, DC, 2014), 1.

[37] Alex S. Wilner and Claire-Jehanne Dubouloz, *Homegrown Terrorism and Transformative Learning: An Interdisciplinary Approach to Understanding Radicalization* (Taylor and Francis Online: Global Change, Peace, and Security 22:1, 2010), 38.

2. User-generated content, such as text posts or comments, digital photos or videos, and data generated through all online interactions, are the lifeblood of social media.
3. Users create service-specific profiles for the website or applications that are designed and maintained by the social media organization.
4. Social media facilitate the development of online social networks by connecting a user's profile with those of other individuals or groups.38

Joint Publication (JP) 3-13, *Information Operation*, refers to Target Audiences as, "an individual or group selected for influence."[39] Terrorists' influence may lead them to various violent activities starting from recruitment to conduct a violent act.

Scope

This research is focused on radicalization through the internet from a Bangladeshi perspective. The socio-cultural environment and demographics of Bangladesh have been taken into consideration. Emphasis has been given to the target audience of Bangladeshi citizens who are vulnerable to these radical ideas. The timeframe of this research is from 1990 through the present day. This research will be qualitative, based on literature review. Additionally, the researcher will interview a few key individuals to ensure a comprehensive analysis of this subject. Complicated technical discussions are outside the scope of this research.

[38] Office of the Joint Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: Government Printing Office, 2012), GL-4.

[39] Ibid.

Limitations

Lack of publicly available information on the radicalization efforts in Bangladesh by various terrorist organizations is a fundamental limitation of this research. There is also a lack of scholarly research in Bangladesh on this subject. Additionally, much of the data on terrorist organizations is For Official Use Only or Law Enforcement Only classification and is not available for use in this thesis.

Another limitation is the policy of the social media companies to release information. Social media like Twitter, Facebook, and YouTube do not disclose any information to the public. Moreover, they rely on user-generated reports to flag content for further investigation. Facebook, for example, will only disclose data to law enforcement on the basis of a valid court order or search warrant. The Government of Bangladesh would need to work with U.S. authorities to obtain information, as Facebook and many other social networks are based in the United States. Facebook states, "We interpret the national security letter provision as applied to Facebook to require the production of only two categories of information: name and length of service."[40]

Delimitations

This research will discuss online radicalization in Bangladesh in generic terms. It will not discuss the cyber-related technical issues in depth. Moreover, it will not discuss any issue that have legal restrictions. This research will be based on content analysis and

[40] Facebook, "Information for Law Enforcement Authorities," Facebook.com, accessed November 1, 2016, https://www.facebook/com/safety/ groups/law/guidelines.

expert interviews. An additional self-imposed constraint was the decision not to attempt to seek information from a radicalized person or group.

Significance of the Study

Many governments recognize the threat posed by violent ideologies spread through the internet. Social media and other communication technologies have enabled the virtual and, in some cases, actual mobilization of dispersed and demographically varied audiences across the world.[41] The characteristics of the social media environment need analysis to counter its usage for spreading radical ideas. According to Twitter's internal statistics, they have approximately 313 million monthly active users with forty-plus languages supported.[42] YouTube claims to have over a billion users, with mobile users averaging forty minutes per viewing session.[43] Facebook estimates having 1.18 billion monthly active users.[44] As per Internet World Stats, Bangladesh has 21 million active Facebook users.[45] Therefore, the internet, particularly social media, provide a wide

[41] Lisa Ferdinando, "Unprecedented Challenge in Countering Adversarial Propaganda," *DoD News*, October 23, 2015, accessed November 1, 2016, http://www.defense.gov/News-Article-View/Article/625750/unprecedented-challenge-in-countering-adversarial-propoganda-official-says.

[42] Twitter, "It's What Happening," Twitter.com, accessed November 1, 2016, https://about.twitter.com/company.

[43] YouTube, "Statistics," YouTube.com, accessed November 1, 2016, https://www.youtube.com/yt/press/statistics.html.

[44] Statistics Brain, "Facebook Company Statistics," Static Brain Research Institute, accessed November 1, 2016, http://www.statisticbrain.com/facebook-statistics/.

[45] Internet World Stats, "Asia Internet Use, Population Data and Facebook Statistics - March 2017," Internet Coaching Library, accessed November 15, 2016, http://www.internetworldstats.com/stats3.htm#asia.

opportunity to terrorists to reach any population in any country. This threat is further grave in countries like Bangladesh where general awareness of the threats paved by the internet radicalization is low, and no comprehensive mechanism exists to prevent the radicalization. In Bangladesh, very few researches have been conducted on radicalization through the internet. A significant void concerning the process of countering online radicalization exists. Therefore, this research will attempt to fill a gap in the scholarly literature by determining an approach to integrate cyber initiatives into the counter-terrorism system of Bangladesh.

CHAPTER 2

LITERATURE REVIEW

The literature review is divided into three sections: understanding online radicalization, online radicalization from a Bangladeshi perspective, and key elements of successful international anti-radicalization programs. Understanding online radicalization will examine the potential power of the internet to influence people. The section on online radicalization from a Bangladeshi perspective will at first, study the terrorists' approach and their target audiences. After that, it will evaluate the existing programs of countering online radicalization. The final section will examine the strategies adopted by the Federal Bureau of Investigation (FBI), The U.S. National Counterterrorism Center (NCTC), Malaysia and Indonesia. The researcher has selected these two countries of Southeast Asia considering religious and cultural similarities, and geographic proximity. This section will assist to determine the key elements of their success that Bangladesh can adopt in future.

Understanding Online Radicalization

The internet has created more opportunities to become radicalized. Many scholarly articles ascribe a role to the internet in promoting radicalization.[46] Those studies suggest that the internet acts as an accelerant and has broken the traditional

[46] Tomas Precht, *Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism* (Copenhagen: Danish Ministry of Defence, 2008), 4.

barriers to radicalize individuals.[47] In this regard, Gabriel Weimann's *Terror on the Internet: The New Arena, The New Challenges* counts the number of websites of terrorist groups and reviews their contents.[48] In his article, Weimann points to the proliferation of extremists' websites. He finds, by the end of 1999 that almost all terrorist groups had established an online presence. Different empirical studies suggest, there is a correlation between extremists' websites and online propaganda, and rapid radicalization.[49]

The reach of the internet has blurred the geographic barriers and connected distant individuals in the virtual world. Peter Neumann, the Director of the International Centre for the Study of Radicalisation, in his research points out that the internet allows terrorists to reach those individuals who would not have been accessible in any other way.[50] For example, Anwar al-Awlaki successfully created online content such as "*Inspire*" that advocates "jihad from home."[51] Through the online instructions, he gradually radicalized and convinced Umar Farouk Abdulmutallab, a young and educated Nigerian, for a

---

[47] Raffaello Pantucci, *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists* (London: International Centre for the Study of Radicalisation and Political Violence, 2011), 34.

[48] Gabriel Weimann, *Terror on the Internet: The New Arena, The New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 15.

[49] Shawn Powers and Matt Armstrong, *Visual Propaganda and Extremism in the Online Environment*, edited by Carol K. Winkler and Cori E. Dauber (Carlisle, PA: The United States Army War College Press, 2014), 166.

[50] Peter R. Neumann, "Options and Strategies for Countering Online Radicalization in the United States," *Studies in Conflict and Terrorism* (2013): 431-432.

[51] Anwar al-Awlaki was a spokesperson and recruiter for Al Qaeda.

"martyrdom mission."[52] Ines von Behr, a senior analyst at RAND Europe, asserts that this kind of online materials have broadened the scope to reach any people, and their appealing contents create more chance to implant radical ideas among the individuals.[53]

The internet creates opportunities to radicalize a wider range of people from all societies. Rachel Briggs and Alex Strugnell, well-known security experts, identify that besides removing the geographic barrier, the internet has erased the social and gender barriers as well to spread extremist ideologies. They highlight that the internet created an opportunity to reach and radicalize women.[54] In many societies, it may be difficult for women to meet personally with male extremists or work with them; it may also be difficult for the women to express certain thoughts in public. However, the internet allows them greater anonymity.[55] Some authors state that the internet benefits the introvert individuals who are seeking the radical ideas by creating the ability to access any content privately.[56] Jerome Bjelopera, a specialist in organized crime and terrorism,

---

[52] Scott Shane, "Inside Al Qaeda's Plot to Blow Up an American Airliner," *The New York Times*, February 22, 2017, accessed March 5, 2017, https://www.nytimes.com/2017/02/22/us/politics/anwar-awlaki-underwear-bomber-abdulmutallab.html.

[53] Ines von Behr, Anaïs Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in The Digital Era* (United Kingdom: RAND Corporation, 2103), 17.

[54] Rachel Briggs and Alex Strugnell, "Radicalisation: The Role of the Internet" (Policy Planners' Network Working Paper, Institute for Strategic Dialogue, London, 2011), 6.

[55] Robert E. Schmidle, "Positioning Theory and Terrorist Networks," *Journal for the Theory of Social Behaviour* 40, no. 1 (2010): 65.

[56] Robyn Torok, "Make a Bomb in Your Mums Kitchen: Cyber Recruiting and Socialisation of White Moors and Home Grown Jihadists" (Conference Proceeding Paper, Australian Counterterrorism Conference, Edith Cowan University, Perth, 2010), 54-55.

says that the characteristics of the internet allow a relative advantage to the terrorists in the present days than in previous generations by fading the lines between countries, societies, and genders.[57] The internet also provides supposed anonymity and a degree of protection and security from detection.[58]

The internet accelerates the process of radicalization. Bjelopera calls the internet an "echo chamber."[59] By this he means, people who are searching any radical ideas to support their thoughts are likely to get some reinforcing content on the internet due to its abundance of storage. The internet is a kind of "one-stop shop" for all the information that individuals may seek to reinforce their pre-existing radical ideas. Therefore, the virtual world reduces the timeframe of radicalization process as opposed to the actual world. Anthony Bergin, a senior research fellow at the Australian National Security College, in his study refers to the internet as a "conveyor belt" that accelerates radicalization by providing an instant and continuous connection to any radical idea.[60] Raffaello Pantucci, the Director of International Security Studies at the Royal United Services Institute (RUSI) in London, further highlights the internet's role in incubating

[57] Jerome P. Bjelopera, *American Jihadist Terrorism: Combating a Complex Threat* (Washington, DC: Congress Research Service, 2011), 101-102.

[58] Weimann, *Terror on the Internet*, 29.

[59] Bjelopera, 101-102.

[60] Anthony Bergin, Sulastri Bte Osman, Carl Ungerer, and Nur Azlin Mohamad Yasin, "Countering Internet Radicalisation in Southeast Asia," Special Report, Issue 22 (Canberra: Australian Strategic Policy Institute, 2009), 5.

and accelerating radicalization.[61] Lieutenant General Robert E. Schmidle Jr. (retired), former U.S. Cyber Command Deputy Director, points that the chat rooms, in particular, are effective for the extremists since they can exchange ideas with like-minded individuals, 24/7, regardless of borders.[62]

The internet allows radicalization to occur without physical contact. Su Yin Yeap and Jenna Park, prominent security experts, explain that the internet enables any individual to access radical religious content from their personal space instead of attending a radical religious gathering.[63] Hence, an individual needs only to have an internet connection, and traveling to other locations is not required. Though the internet reduces hurdles to interaction, a few scholars argue that person to person human interaction is necessary for radicalization. However, Behr says, in a digital era online activities may be considered as an extension of real lives, and a direct physical connection is no longer essential.[64] Besides the actual world, personal relationships may grow in the virtual world. Thus, Mitchell Silber and Arvin Bhatt, intelligence analysts of the New York Police Department Intelligence Division, assert that radicalization on the internet is not necessarily any different to what would happen with other more private

---

[61] Pantucci, *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists*, 3-4.

[62] Schmidle, 65.

[63] Su Yin Yeap and Jenna Park, *Countering Internet Radicalisation: A Holistic Approach* (Singapore: S. Rajaratnam School of International Studies, 2010), 2.

[64] Behr et al., 20.

and less visible sources.[65] Besides, the internet increases opportunities for self-radicalization. It is a process where an individual gradually becomes radicalized by himself.[66] Hence, the internet creates opportunities for radicalization without face to face human interaction.

The U.S. Joint Publication 3-12 (R), *Cyberspace Operations*, describes the concept of cyber-persona and challenges in targeting those. The cyber-persona layer is a digital representation of an individual or identity in cyberspace.[67] It consists of the people actually on the network, and may directly link to an actual person or entity.[68] Moreover, a single cyber-persona can have multiple users. For example, a single person can have multiple accounts on various websites that create many cyber-persona. On the other hand, several people may share a single account, thereby, making a single cyber-persona. Consequently, ascribing responsibility and targeting in cyberspace is difficult.[69] An extremist can adeptly exploit the characteristics of cyber-persona and evade interception by LEAs.

---

[65] Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat" (Report, The New York City Police Department, New York, 2007), 16.

[66] "Studies into Violent Radicalisation; Lot 2: The Beliefs Ideologies and Narratives" (Study Paper, Directorate General Justice, Freedom and Security, European Commission, UK, 2008), 89.

[67] Office of the Joint Staff, JP 3-12 (R), *Cyberspace Operations*, I-3.

[68] Ibid., I-4.

[69] Ibid.

An individual moves through several phases as he becomes radicalized. In a New York Police Department (NYPD) radicalization case study, Silber and Bhatt identify four phases of radicalization: pre-radicalization, self-identification, indoctrination and jihadization.[70] The case study recognizes the impact of the internet on an individual who is looking for "a religious identity and a cause."[71] The internet facilitates each of the stages to instruct, socialize, indoctrinate and recruit.[72] The FBI has also created a radicalization model similar to that of the NYPD. The FBI model has four stages: pre-radicalization, identification, indoctrination and action.[73]

Fathali M. Moghaddam, an American psychologist in Georgetown University, uses the metaphor of a "staircase" leading to the terrorist act while describing the gradual process of radicalization.[74] The staircase has a ground floor and five higher levels; each level has its specific psychological characteristics. The internet may contribute at each level leading to terrorism.[75] He says that often a feeling of deprivation or unfair social treatment initiates the process. However, only a few people climb the stair and finally get recruited in the terrorist organizations. They think that they have no active voice in the

[70] Silber and Bhatt, 6-7.

[71] Ibid., 8.

[72] Ibid., 8-9.

[73] Ibid., 30.

[74] Fathali M Moghaddam, "The Staircase to Terrorism, a Psychological Exploration," *American Psychologist* 60, no. 2 (2005): 161-162.

[75] Ibid.

society, and terrorist leaders motivate them in adopting aggressive actions as legitimate tools.[76] Figure 1 illustrates the Moghaddam's staircase to radicalization.

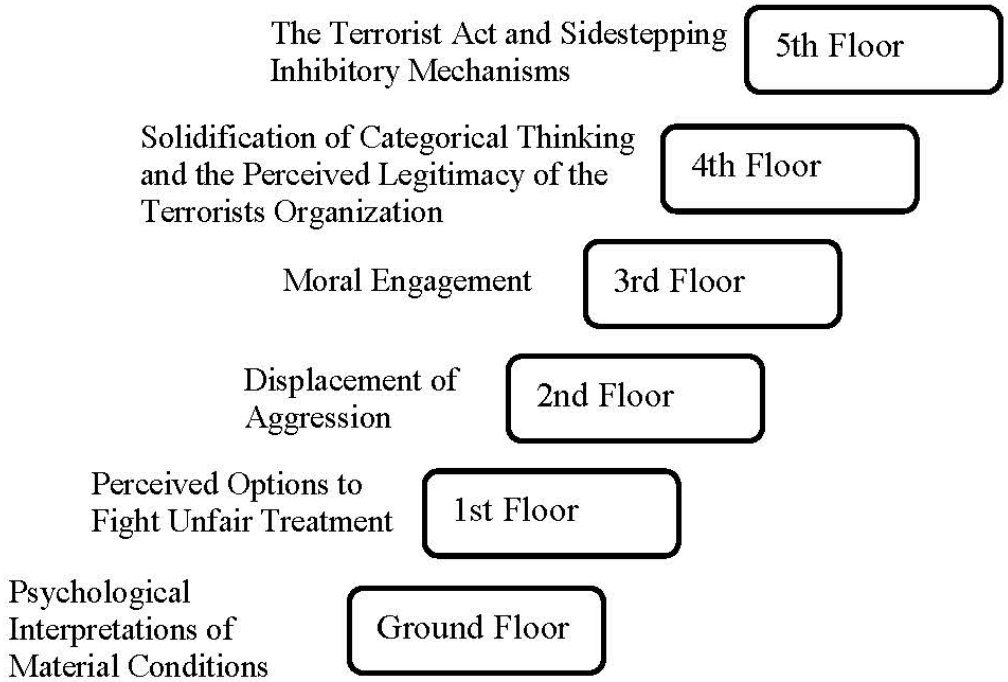

Figure 1. Moghaddam Staircase to Radicalization

Source: Fathali M Moghaddam, "The Staircase to Terrorism, a Psychological Exploration," *American Psychologist* 60, no. 2 (2005): 161-169.

[76] Ibid.

Online Radicalization from a Bangladeshi Perspective

Terrorists' Approach and their Target Audience

In Bangladesh, a few religion-based terrorist organizations have gained capabilities to develop and spread their radical messages online.[77] They have attracted public and media attention through terrorist activities and propaganda. Besides, a few leftist political groups are also trying to develop their online capabilities.[78] At present 13 terrorist organizations are operating actively, and 29 others are operating covertly using fake credentials.[79] The Special Branch (SB) of Bangladesh Police has provided the names of eight terrorist organizations to Home Ministry who are very active on the internet: Ansarullah Bangla Team, Allah'r Dal, Islamic Solidarity Front, Tamiruddin Bangladesh, Tawhidee Trust, Hizbut-Tawhid, Shahdat-e-Nabuwat and Jamat-as-Sadat. The government has already banned five of these terrorist organizations, and likely to ban eight more in future.[80] In the future, these groups are likely to continue enhancing their online capabilities.

Bangladeshi terrorist groups appear to be active on the internet, particularly on Facebook and YouTube, spreading their radical philosophy. Spreading propaganda through the internet is safer because it has a lower possibility of being tracked by LEAs. Farooq notes that the online propaganda of the terrorists in Bangladesh have become

---

[77] Sobhan, *The Role of Civil Society in Countering Radicalization in Bangladesh*, 13.

[78] Ibid., 7.

[79] Ibid., 8.

[80] Ibid.

more organized and appealing to their targets.[81] For example, Tanbir Uddin Arman, a Bangladeshi researcher on security issues, claims that the terrorists try to exploit the ethnoreligious sentiment of the people while developing their messages, and appeal to their beliefs to embed their radical ideas.[82]

Over the last few years, hate speech and violent ideology have triggered a number of terrorist attacks and incidents of communal violence in Bangladesh. The appeal of such messages on the internet was evident in the Ramu and Pabna incidents where agitated people attacked religious minorities. In both cases, doctored photos and messages on the Facebook defaming Islam, posted by unknown persons using pseudonyms, agitated people.[83] The photos and messages denigrate the Prophet and Mecca which is unacceptable by the Muslim Bangladeshi people in general.[84] It is evident that the unknown persons intentionally hurt the religious sentiment of the people to foment communal violence in the society. Social media has, therefore, become an easy method to spread radical ideas in Bangladesh.

The terrorists in Bangladesh attempt to build their radical narratives based on religious and socio-political issues. Moghaddam identifies that a number of reasons can

---

[81] Ibid., 13.

[82] Arman.

[83] Ibid.

[84] Ahmed Humayun Kabir Topu, "Hindus attacked in Pabna," *The Daily Star*, November 3, 2016, accessed March 6, 2017, http://www.thedailystar.net/news/hindus-attacked-in-pabna.

potentially trigger the radicalization such as ideology, social deprivation, and poverty.[85] These triggers may be different for different classes of the society, and terrorists adeptly attempt to exploit those. Nirmal Ghosh, a security analyst and the senior correspondent for *The Straits Times*, states that though Bangladesh is politically a secular country, terrorists appeal to the Muslim majority population for making it an Islamic state under Sharia law.[86] They seem to exploit and trigger the religious sentiment of the people. These groups intentionally create fake photos with radical messages such as the prosecution of Muslim Rohingyas and spread those on social media to incite communal violence in the country.[87] Furthermore, the extremists adeptly construct radical narratives on socio-economic disparity and political issues to create sympathizers.

Bangladeshi youths are particularly vulnerable to online radicalization due to lack of awareness. In Bangladesh, the affluent and educated youths have more access to the internet than the poor. This increases the chance of radicalization by triggering their ideology, mostly religious, without any face to face interaction. Therefore, Farooq in his study suggests, the Bangladeshi terrorists seem to target the educated youths by spreading

---

[85] Moghaddam, 161-162.

[86] Nirmal Ghosh, "Battle for Bangladesh's Soul as Islamic Radicals Push for Power," *The Strait Times*, August 2, 2016, accessed February 21, 2107, http://www.straitstimes.com/opinion/battle-for-bangladeshs-soul-as-islamic-radicals-push-for-power.

[87] Tuhin Shubhra Adhikary and Wasim Bin Habib, "Fake Photos Trolling," *The Daily Star*, November 26, 2016, accessed February 21, 2107, http://www.thedailystar.net/frontpage/fake-photos-trolling-1320613.

appealing messages on the Internet.[88] A study on 250 detained militants in Bangladesh revealed that almost 82 percent of them were radicalized through various social media.[89] Surprisingly, only 22 percent of them are from madrasa background while others are from general education.[90]

Bangladeshi Counter-Radicalization Programs

The Government of Bangladesh has implemented several plans and strategies to counter radicalization in the country. However, Abul Kalam, a well-known Bangladeshi security expert, argues that the government has mostly applied coercive methods to minimize the terrorist threats.[91] Aynul Islam, a research officer at Bangladesh Institute of International and Strategic Studies (BIISS), in his article categorizes the government initiatives into two types: operational drives by law and security forces, and legal actions.[92] The law enforcement agencies have achieved some success in disrupting a few of the extremist groups. Many extremist leaders and activists have been arrested and put

---

[88] Sobhan, *The Role of Civil Society in Countering Radicalization in Bangladesh,* 10.

[89] Kamrul Hasan, "82% Bangladeshi Militants Radicalised Through Social Media," *Prothom Alo*, March 24, 2017, accessed April 3, 2017, http://en.prothom-alo.com/bangladesh/news/143243/82%25-Bangladeshi-militants-radicalised-through.

[90] Ibid.

[91] Abul Kalam, "The Challenges of Terrorism: Bangladesh Responses," in *Responding to Terrorism in South Asia*, ed. S. D. Moni (Monohar, New Delhi, 2006), 147.

[92] Aynul M. Islam, "Mapping Terrorism Threats in Bangladesh," *Bangladesh Institute of International and Strategic Studies* 29, no. 2 (April 2008): 165.

on trial. However, different online activities suggest that few of their followers are still covertly maintaining their footprints on the internet.

Bangladesh faces challenges to monitoring the spread of radical content through cyberspace. The Bangladesh National Telecommunication Monitoring Centre (NTMC) monitors suspicious online and cell phone related activities to help intelligence and law enforcement agencies. However, it has outdated technology and lacks the capacity to control the modern ICT.[93] The government effort to shut down or censor a few websites seems not very effective because extremists can innovate new ways to reach people. Moreover, it is hard to identify and stop secret groups on social networking sites that contain radical ideas.

The Government of Bangladesh has enacted some legislation to ensure cyber security. Bangladesh Telecommunication Regulatory Act 2001, The ICT Act 2006, Digital Security Act 2016 (Draft) are the important legislation of Bangladesh in this regard.[94] The Bangladesh Telecommunication Act 2001 establish the foundation of cyber-related laws and makes some of the cybercrimes punishable. For example, it articulates the punishment for activities leading to breach of national security and abusive usage of websites using telecommunications equipment.[95] Section 53 of this Act gives

[93] Rejaul Karim Byron, "Bangladesh to Purchase Modern Surveillance Equipment," *The Daily Star*, August 3, 2015, accessed March 14, 2017, http://www.thedailystar.net/frontpage/govt-buy-new-surveillance-tools-120967.

[94] Md. Mahboob Murshed, "A Comparative Analysis between Bangladeshi and Korean Legal Frameworks for Combating Cybercrime to Ensure Cyber Security," *Korean University Law Review* 19, no. 23 (2016): 30.

[95] Ibid., 32-33.

the telecommunication authority ample power to intercept the communication system to stop any unwanted cyber incidents with the use of telecommunication tools in the country.[96] However, these penal provisions do not directly address the issues of cybercrimes.[97]

The ICT Act 2006 provides a more detailed legal framework to combat cybercrimes. In this Act sections 56,57,66,67, and 68 describe the manner and the offenses related to cyber. Though this law establishes a Cyber Tribunal and Cyber Appellate Tribunal, it does not define the term "cybercrime."[98] Under section 57 of this Act, the court can sentence violators up to 14 years in prison for willfully publishing any fake, obscene or defaming information on the internet that may be harmful to the society.[99] However, the Tribunal's effectiveness is limited because it cannot take cognizance of any offense either on its own or on the basis of a complaint from an individual. It can work only after a written report from a Police Officer.[100] Md. Mahboob Murshed, an advocate in the Supreme Court of Bangladesh, says that this provision makes the law less effective in combating cybercrimes. This law seems archaic and not

[96] Bangladesh Telecommunication Regulatory Commission, *The Bangladesh Telecommunication Act 2001*, 53.

[97] Murshed, 33.

[98] Ibid., 30.

[99] Bangladesh National Parliament, *The Information and Communication Technology Act 2006*, 16.

[100] Ibid.

compatible with the technical and forensic issues of investigating and prosecuting a cybercrime.[101]

The Digital Security Act 2016 (Draft) will be an upgraded version of the cyber-protection law of the country. It is expected to replace some of the controversial provisions of cybersecurity laws, like section 57 of the ICT Act 2006. However, the government has not yet addressed the procedural problem of the Tribunals mentioned in the case of the ICT Act 2006.[102] It is also harshly criticized by the journalists for the possibility of impinging freedom of speech.[103]

Islam says that several agencies are operating in Bangladesh for combating terrorism, but their capabilities and activities are not well coordinated.[104] The Bangladesh Police, the Rapid Action Battalion (RAB), Border Guard Bangladesh, armed forces and intelligence agencies are mainly responsible for fighting terrorism. Though these forces have counter-terrorism cells, they work separately. He further argues that the police are not well equipped and trained to deal with the new trends of online terrorism. On the other hand, several intelligence agencies in Bangladesh such as the National Security Intelligence (NSI), the Directorate General of Forces Intelligence (DGFI), Special Branch

[101] Murshed, 1.

[102] "Digital Security Act 2016 (Draft)," accessed February 27, 2017, https://www.forum-asia.org/uploads/wp/2016/08/Digital-Security-Act-English-09.03.2016.pdf.

[103] Committee to Protect Journalists, "Proposed Cyber-Security Bill Threatens Media Freedom in Bangladesh," CPJ.org, August 24, 2016, accessed March 6, 2017, https://cpj.org/2016/08/proposed-cyber-security-bill-threatens-media-freed.php.

[104] Islam, 165.

(SB) of Police and the RAB Intelligence Wing are working to identify potential threat sources. In May 2004, NSI constituted a separate body called "counter-terrorism cell" to identify particular risk populations and areas, and threat groups. The "Counter-terrorism Bureau" of DGFI has been working to evaluate, analyze, and frame counter-terrorism policy at strategic and operational levels.[105] Nonetheless, there is no set mechanism through which the agencies can share information and coordinate their collection efforts. The absence of an overarching organization causes a lack of coordination among the agencies of Bangladesh.[106]

Islam in his article, *Mapping Terrorism Threats in Bangladesh*, identifies a few key deficiencies of Bangladeshi programs to prevent radicalization.[107] First, Bangladesh has no set mechanism to monitor the internet for preventing the spread of radical ideas. There is a lack of knowledge and understanding of the threats that can spread through cyberspace. The country has neither sufficient technological and organizational expertise nor functional international partnerships for capacity building. Second, the law enforcement agencies do not have close links with the other service sectors or the private sector to identify suspicious activities. Third, the Government of Bangladesh is not sufficiently addressing strategic issues like de-radicalization and counter-ideology. Fourth, there is a very limited initiative to educate professional groups like academics, the media, service sector officials, and political leaders to create general awareness.

---

[105] Sakhawat M. Hussain, *Capacity Building of Law Enforcement and Intelligence Agencies,* ed. Farooq Sobhan (Dhaka: University Press, 2008), 70.

[106] Islam, 165.

[107] Ibid., 167-168.

There are almost no community-based programs in the country for developing cyber awareness. Fifth, the government overemphasizes coercive approaches in dealing with terrorism issues. There is no dedicated research institution in the government to provide a forum for understanding and research on critical issues of online radicalization. Although the counter-terrorism bureau of DGFI is responsible for policy related activities, it is barely possible to formulate a viable strategy by a body of armed forces alone. Finally, he claims that the Bangladeshi plans and policies are highly bureaucratic, ambiguous, and unaccountable.[108]

Key Elements of Successful Anti-Radicalization Models of Different Countries

The Strategy of the Federal Bureau of Investigation (FBI)

There are multiple counterterrorism agencies in the United States with their defined roles. This research will discuss the strategy of the FBI to prevent online radicalization since it focuses on countering internal threats. According to the FBI official website, its activities are of three categories: deterring the producers of online radical ideas, empowering online communities, and reducing the demand for radical ideologies.[109]

The FBI's current programs deter producers of extremist materials and create a more challenging environment for radical messages. As a federal law enforcing agency (LEA), the FBI directly takes action against extremists in the U.S. It has a well-developed

[108] Ibid.

[109] FBI, "Countering Violent Extremism," accessed December 15, 2016, https://www.fbi.gov/news/stories/countering-violent-extremism.

cyber monitoring system. The Internet Crime Complaint Center (IC3) provides the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning any suspicious activities. Moreover, the Cyber Action Team and National Cyber Forensic and Training Alliance enhances its cyber capabilities.[110]

The FBI implements the government's policies and conducts various community-based activities to create a general awareness. The U.S. National Security Strategy 2010 articulates, "Our best defenses against this threat (radicalized people) are well informed and equipped families, local communities, and institutions. The Federal Government will invest in intelligence to understand this threat and expand community engagement and development programs to empower local communities."[111] In connection to this, the FBI is one of the lead agencies to implement the 2011 White House strategy - "Empowering Local Partners to Prevent Violent Extremism in the United States."[112]

The FBI shares information with partners, provides assessments on radicalization, cooperates with other LEAs, and assists communities in building awareness. For example, it conducts the Community Resilience Exercise (CREX) with several partners in local communities. This exercise promotes awareness in the society by gaining a better

[110] FBI, "Cyber Crime," accessed December 15, 2016, https://www.fbi.gov/investigate/cyber.

[111] The White House, *National Security Strategy 2010* (Washington, DC: The White House, 2010), 19.

[112] The White House, *Empowering Local Partners to Prevent Violent Extremism in the United States* (Washington, DC: The White House, 2011).

understanding of the issues related to radicalization. Based on this exercise, the FBI also suggests action plans to LEAs and social actors to combat radicalization.[113]

The FBI works to reduce the appeal of extremist messages by launching various youth programs.[114] The aim of these websites is to promote cybersecurity awareness among the youths so that they do not fall into the trap of extremists' appealing messages. For example, "Don't Be a Puppet: Pull Back the Curtain on Violent Extremism" is an interactive website developed by the FBI for promoting awareness among the youths. Such awareness programs help to strengthen youth's resistance to radicalization and possible recruitment.

Moreover, the FBI seems to maintain transparency during investigations that bolster the democratic rights of the people. *The New York Times* has revealed the investigation case of Mr. Abdulmutallab – A Nigerian Al-Qaeda activist who attempted to blow up an American airplane in 2009. Anwar al Awlaki radicalized and inspired him for this "martyrdom mission," but he failed to detonate on board due to a malfunction of the explosives. The FBI thoroughly investigated him, while maintaining transparency and respect for human rights. The agency even flew his relatives to the U.S. to encourage him to talk and cooperate. The FBI's interrogation techniques proved to be effective to gain willing cooperation of Abdulmutallab and discern valuable information. Though initially

[113] FBI, "A New Approach to Countering Violent Extremism: Sharing Expertise and Empowering Local Communities," accessed December 21, 2017, https://leb.fbi.gov/2014/october/a-new-approach-to-countering-violent-extremism-sharing-expertise-and-empowering-local-communities.

[114] FBI, "Countering Violent Extremism," accessed December 15, 2016, https://www.fbi.gov/news/stories/countering-violent-extremism.

they kept the investigation details secret, later they released unclassified information to the public. This example demonstrates the FBI's commitment to maintaining transparency and people's access to information.[115]

The Role of the U.S. National Counterterrorism Center (NCTC)

The United States founded the NCTC in August 2004 to coordinate and integrate the intelligence and counterterrorism efforts of different agencies.[116] It is a subordinate component to the Director of National Intelligence. This agency serves as an apex body for planning U.S. counterterrorism activities and integrating all instruments of national power. Unlike the FBI, it primarily focuses on international issues.[117] Key functions of the NCTC includes analyzing and integrating all intelligence on terrorism and counter-terrorism, conducting strategic and operational planning, and assigning responsibilities to the lead governmental agencies in countering terrorism.[118] The major sub-organizations of the NCTC, depicted in figure 2, are the information sharing and knowledge development department, the plans and administration department, the current support

---

[115] Scott Shane, "Inside Al Qaeda's Plot to Blow Up an American Airliner," *The New York Times*, February 22, 2017, accessed February 23, 2017, https://www.nytimes.com/2017/02/22/us/politics/anwar-awlaki-underwear-bomber-abdulmutallab.html?_r=0.

[116] Office of the Director of the National Intelligence, "The National Counterterrorism Center," accessed February 19, 2017, https://www.nctc.gov/overview.html.

[117] Brian R Reinwald, "Assessing the National Counterterrorism Center's Effectiveness in the Global War on Terror" (Research, US Army War College, Carlisle, PA, 2007), 1.

[118] Ibid., 7.

and requirements department, and the directorate of strategic operational planning.[119] The intelligence directorate integrates intelligence among different agencies. The strategic operational planning directorate focuses on strategic planning, governmental role delineation, and monitoring. It "fills the gap between policy, strategy development, and the execution of counterterrorism operations."[120]

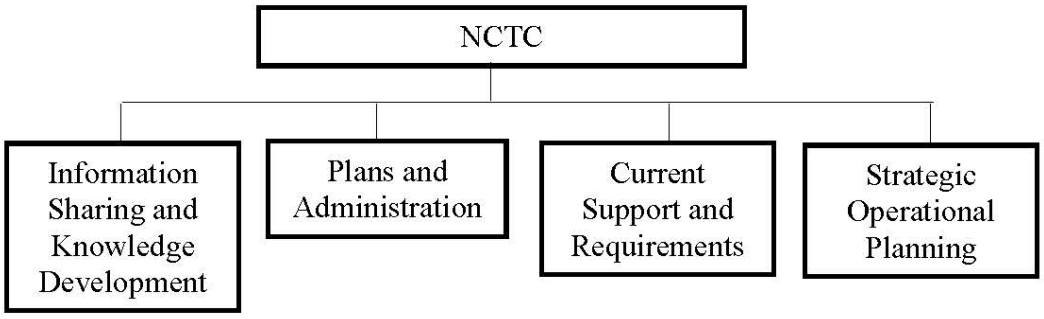

Figure 2. Organization of NCTC

Source: Researcher's Construct Based on the National Counter Terrorism Center website.

The NCTC is an overarching agency to evaluate and suggest counter-terrorism policies to the government. As per the NCTC official website, it has five main objectives: (1) fulfill leadership role in the counterterrorism community; (2) ensure domestic and foreign partners' access to terrorism information and analysis as required; (3) attract, develop, and reward a highly skilled workforce; (4) advance business practices to improve NCTC's culture of collaboration, communication, and integrity, and (5) enhance

[119] Ibid., 9.

[120] Ibid., 9-10.

the use of information technology resources to strengthen NCTC's core capabilities.[121] It has partnerships with different agencies, including the Central Intelligence Agency (CIA), FBI, the Department of Justice, the Department of State, the Department of Homeland Security, and the Department of Defense. The NCTC also evaluates the effectiveness and training of other counter-terrorism agencies of the USA.

The NCTC serves as the primary organization of the United States Government for integrating various agencies. It synchronizes almost 30 different agencies to facilitate rapid information sharing and collaborates with foreign partners. It serves as the government's central information bank on terrorist organizations. Moreover, The NCTC is a key player in the Office of the Director of National Intelligence's Homeland Threat Task Force.[122] It assigns responsibilities to various departments and agencies but does not direct the execution of any operations. It helps the partner agencies to fulfill their missions by sharing information and assessments. For example, the NCTC maintains several databases such as Terrorist Identities Datamart Environment, NCTC Online, and NCTC Online CURRENT for enhancing collaboration among various agencies. Moreover, the NCTC's Interagency Threat Assessment and Coordination Group allows information sharing between the intelligence communities.[123]

---

[121] The National Counterterrorism Center, "Who We Are," accessed February 14, 2017, https://www.nctc.gov/strategicintent.html.

[122] Ibid.

[123] Information Sharing Environment, "The Joint Counterterrorism Assessment Team (JCAT)," accessed February 14, 2017, https://www.ise.gov/interagency-threat-assessment-and-coordination-group-itacg.

Malaysian and Indonesian Strategy

Two Southeast Asian countries- Malaysia and Indonesia- seem to be quite successful in fighting against radicalization. Kumar Ramakrishna, a distinguished Southeast Asian security analyst, states that Malaysia and Indonesia have adopted "bottom-up" indirect strategy against online radicalization.[124] Bangladesh has many commonalities in culture with Indonesia and Malaysia. Their counter-radicalization strategies include culture-based approaches, effective counter-messaging, and integrating Muslim scholars for countering propaganda.

Malaysian and Indonesian counter-radicalization strategy focuses attention on certain aspects of their culture like sympathy to Islamic messages. They have adopted a culture-based approach to formulating an indirect strategy.[125] Ramakrishna states that Kuala Lumpur guides the activities of LEAs and other government agencies to promote an overall positive message in the society. They also systematically audit their policies and activities so that physical actions do not contradict with the government's positive messages. These countries effectively engage media and religious forums. As a result, the radical Islamists were not successful in spreading propaganda in these countries.[126]

The second strategy of these countries may be called "Divide and Conquer" by compelling counter-messaging. Their counter-messaging is not only reactive to

---

[124] Kumar Ramakrishna, "The Southeast Asian Approach to Counter-Terrorism: Learning from Indonesia and Malaysia," *The Journal of Conflict Studies* (Summer 2005): 28.

[125] Ibid.

[126] Ibid., 40-41.

extremists' propaganda but also proactive. In Malaysia, the Psychological Warfare Section led by Tan Sri Dato C.C. Too always tries to split the extremists from their leaders. These efforts focus on counter messaging highlighting and emphasizing the weakness of the radical leaders.[127] They deliberately try to drive a wedge between the leaders and the followers. In Pakistan, for instance, it is known that many jihadi leaders live luxuriously, while the workers are extremely vulnerable.[128] Moreover, the terror attacks in Saudi Arabia, Turkey, and Indonesia produced numerous Muslim casualties. The Psychological Warfare Section leverages such examples while creating counter-narratives. They explain on websites and in the media how extremist leaders have exploited their status.

Indonesia and Malaysia have also evolved a concept of "fight fire with fire" to combat radicalization. They have derived this strategy from their long history of counterinsurgency. During that period, they used to employ the Chinese residents in the countries to prevent recruitment to the Chinese communist guerrilla groups.[129] In today's context, they use progressive Islamic scholars in a counter-propaganda role. The countries have large numbers of learned Islamic scholars who can be employed in this role such as Azyumardi Azra, Bahtiar Effendy, Nurcholish Madjid, and Abdurrahman

---

[127] Kumar Ramakrishna, *Emergency Propaganda: The Winning of Malayan Hearts and Minds 1948-1958* (UK: Psychology Press, 2002), 113-118; 198-199.

[128] Jessica Stern, *Terror in the Name of God: Why Religious Militants Kill* (New York: Harper Perennial, 2004), 136.

[129] Ramakrishna, 212-13.

Wahid. They are quite capable of constructively engaging people at home and abroad.[130] Indonesia and Malaysia also promote open debate within the Muslim community. A constructive discussion appears to foster greater critical thinking and act as an antidote to radicalization.[131]

The International Multilateral Partnership against Cyber Threats (IMPACT) is located in Cyberjaya, Malaysia, and is designed as the country's leading cyber-threat integration center. It is also a training and skill development center for all related agencies. Its Global Response Center assists member countries in the early identification of cyber-threats and provides guidance on necessary remedial measures. The Global Response Center is partnered with leading software companies like Microsoft, Symantec and Kaspersky Labs. Besides the academic network, IMPACT provides members with access to specialized ICT laboratories, specialized equipment, resource centers and other facilities.[132] This center analyzes the present and future trends of cyber threats including online radicalization and suggests the governments for policy formulation. Therefore, it acts as a premiere agency to develop and share key capabilities for countering online radicalization.

---

[130] Karim Raslan, "The Moderate Majority," *Time Asia*, October 28, 2002, accessed February 14, 2017, http://www.time.com/time/asia/magazine/article/0,13673,501021028-366388,00.html.

[131] Ministry of Home Affairs, "The Jemaah Islamiyah Arrests and the Threat of Terrorism" (White Paper, Ministry of Home Affairs, Singapore, January 7, 2003), 17.

[132] International Multilateral Partnership Against Cyber Threats, "Impact Overview," accessed November 15, 2016, http://www.itu.int/ITU-D/conferences/rpm/2009/asp/documents/IMPACTOverview.pdf.

Summary

This literature review suggests that the internet has an influential role in radicalization, and authors have termed the internet to be ‘facilitative’ or ‘reinforcing’ or an ‘accelerant’ of radicalization. Literature on online radicalization have followed four main themes:

1. The internet increases opportunities to become radicalized.
2. The internet accelerates the radicalization process.
3. The internet enables radicalization to occur without person to person contact.
4. The internet increases opportunities for self-radicalization.

Radicalization through the internet is a grave concern for Bangladesh. Some terrorist groups in Bangladesh might have virtual connections with global terrorist organizations like ISIL and Al-Qaeda. These groups have gained cyber expertise to spread their ideologies. Educated youths, especially, have become lucrative targets for the extremists. The terrorists attempt to exploit the religious sentiment of the people through social networking sites. Their doctored messages have triggered a number of terrorist attacks and episodes of communal violence across the country.

In response, Bangladesh has mainly pursued coercive or negative measures to prevent online radicalization. These actions may be divided into three categories: legal actions, content filtering, and restricting access. The government has already enacted cyber-related legislation, and a few more laws are still in draft form. It has already implemented laws against the producers of radical messages. The NTMC is primarily responsible for monitoring online activities and filtering content; however, it has a limited technology. At times the Government of Bangladesh has restricted access to some

websites that contain radical messages. This effort seems ineffective because many people used proxy servers to bypass the government restriction. Bangladesh has many LEAs operating against terrorism such as Police, RAB, and SB, but their efforts are fragmented due to lack of a coordinating authority. Moreover, all related agencies in the country may face challenges in maintaining updated cyber expertise concerning terrorist groups. Chapter 4 will evaluate the Bangladeshi efforts to prevent online radicalization in greater details.

Many countries across the globe have developed successful programs to counter radicalization through cyberspace. Engagement and synchronization of activities appear to be the cornerstone of most of the successful models. These models integrate both positive and negative measures, emphasizing the positive. The FBI's community-based engagements are instrumental in developing awareness among the youths in the U.S. On the other hand, the U.S. NCTC is an overarching body that coordinates all agencies and instruments of national power to fight terrorism.

In Southeast Asia, Malaysia and Indonesia seem to be quite successful in preventing online radicalization. They have adopted a culture-based soft approach including effective counter-messaging and awareness programs. Moreover, the IMPACT, located in Malaysia, acts as the leading center for combating cyber threats. It facilitates international collaboration for capacity building and information sharing. Chapter 4 will identify the key elements of these models that Bangladesh might adopt.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter explains the research methodology to organize the information of reviewed literature. It enables a systematic analysis while answering the research questions related to the problem identified. In chapters 1 and 2, this research introduces the readers to the background of the problem and related key literature. It assists the readers in capturing the framework of the problem to understand the analysis of chapter 4. The research methodology presented in this chapter provides the reader with the linkage between the background material and the analysis.

Overview of the Approach

This research is based on a qualitative analysis. Figure 3 illustrates the flow of research methodology. The primary question attempts to provide a "binary answer" about the effectiveness of counter-radicalization programs of Bangladesh. The secondary questions are the stepping stones to the primary question. The first secondary question will determine the Bangladeshi measures to prevent online radicalization. The second question will identify the key elements of successful programs of other countries. Therefore, comparing the two secondary questions, the researcher determines the gaps of Bangladeshi programs in order to answer the primary question. Thereafter, the third secondary question attempts to inform the Government of Bangladesh on how to develop an effective counter-radicalization program. The suggestions will be based on the effective aspects of other countries' programs determined previously.

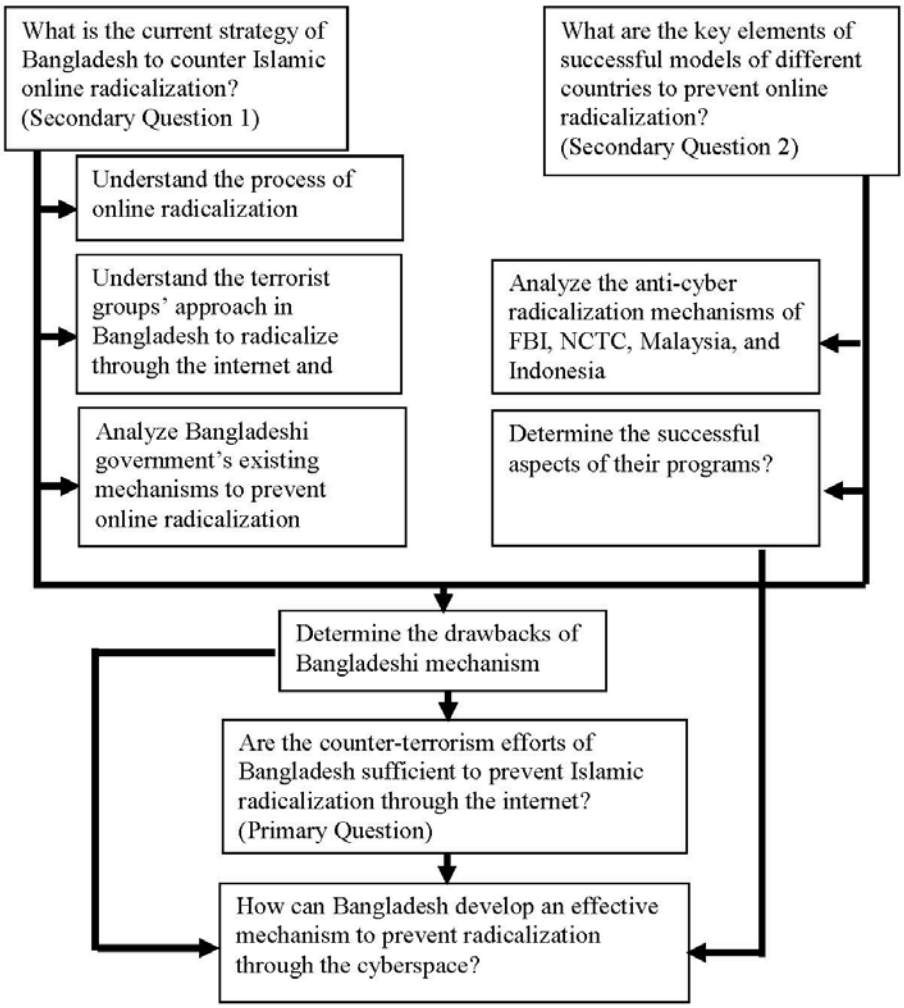

Figure 3. Overview of the Research Methodology

Source: Researcher's Construct.

Data Collection

This research primarily depends on content analysis of various scholarly articles. The researcher uses many unclassified, open-source information from books, periodicals, journals, newspapers, research papers, and keynote papers for conducting this research. Internet articles remain as a major source of data since it provides easy access to an abundance of scholarly articles.

The researcher synthesizes literature reviews and expert opinions to answer the research questions. First, he reviews existing key literature to identify major themes related to the internet radicalization. It consists of a systematic search and review of the literature that includes specific terms, the link between internet and radicalization, and existing counter-terrorism efforts of Bangladesh. The researcher uses a number of scholarly articles in concert with the internet resources to understand the role of the internet in radicalizing people. Second, he interviews an active duty military officer and an academician to understand their views. Such stakeholder engagement allows him to narrow down the literature for review through the identification of key documents, issues, and challenges. The researcher follows all existing academic policies and maintains ethical obligations while interviewing the scholars.

Limitations of Data Collection

First, primary and classified data in connection to this research are not publicly available. Therefore, this study attempts to synthesize the key arguments of the reviewed literature with expert opinions. Second, most of the open source information contain biases or reflects a set perspective. However, the researcher uses a number of sources and cross-matches those in an attempt to minimize biases and preconceived ideas. Last, considering the intended audiences, this research intentionally keeps the cyber-related technical aspects at a minimal level. It discusses the technical aspects in broader terms for general understanding.

CHAPTER 4

ANALYSIS

This chapter analyzes the Bangladeshi counter-radicalization effort to answer the primary research question. The researcher will conduct the analysis based on the literature reviewed in chapter 2 and the result of two interviews. The first section of this chapter summarizes the seemingly effective elements of the FBI, NCTC, and country-based counter-radicalization efforts. In the second section, it analyzes the Bangladeshi counter online radicalization mechanisms to evaluate its effectiveness in the present context. After that, it provides the Government of Bangladesh a few measures to develop a more comprehensive model to prevent online radicalization. Moreover, the researcher personally interviewed two key respondents – an active duty military officer and an academician. This chapter summarizes their opinions and incorporates these into the analysis.

Analysis of the Successful Counter-Radicalization Models

Chapter 2 discusses various successful counter-radicalization models in detail. It unveils a few significant aspects contributing to their success. These elements can be broadly categorized into 3 parts:

1. Reducing supply of radical ideas on the internet.
2. Reducing demand for the radical ideas to the general people.
3. An organizational approach to implementing the measures.

These approaches are not standalone; the countries and the agencies discussed in chapter 2 – Indonesia and Malaysia, and the FBI and NCTC in the USA - employ all elements of national power to synchronize them. The significant aspects are highlighted in table 2:

Table 2. Key Elements of Successful Counter-Radicalization Mechanism

Country/ Agency	Key Elements
FBI	• Broad activities are: deterring the producers of online radical ideas, empowering online communities, and reducing the appeal of radical ideologies • Sophisticated cyber monitoring system • Active and easily accessible cyber-crime complaint centers like Internet Crime Complaint Center (IC3) • Engages local communities and schools to develop cyber awareness • Conducts Community Resilience Exercise • Maintains interactive websites to generate awareness among youths • Initiates community-based youth programs • Maintains transparency and ensure human rights during any investigation.
NCTC	• Apex agency for planning and integrating the USA counterterrorism efforts • Strategic and operational level planning • Evaluates training, capacity, and actions of all other agencies • Integrating and sharing intelligence with all partners • Maintains a central database • Provides assessment to other agencies • Suggests government for policy formulation
Malaysia and Indonesia	• Culture-based soft approach • Effectively engages media, cultural and academic forums • Integrating Islamic scholars for preparing and promulgating counter-narratives (fight fire with fire) • Counter-messaging is not reactive to extremists' propaganda; rather the Malaysian Psychological Warfare Section deliberately attempt to drive a wedge among extremist leaders and followers by counter-narratives • IMPACT works as the lead cyber threat integration center in Malaysia • The governments tries to ensure the rule of law and maintain transparency in their activities

Source: Researcher's construct based on various literature reviewed in chapter 2.

Synthesizing the key elements, the models discussed above offer a few key insights for combating online radicalization. The FBI and NCTC of the United States, and Indonesia and Malaysia appear to develop their technological and intelligence gathering capabilities continuously. The U.S. system utilizes a unified approach under a coordinating agency, required for combating radicalization. The maintenance of a central database with the provision of shared access enhances the law enforcement agencies' effectiveness. Similarly, Malaysia has a well-developed research center that analyzes trends of radicalization and informs the government on various policy matters. Considering the dynamic nature of the virtual world, it seems difficult for a country to prevent radicalization by itself. The virtual world is not limited by a country's geographic boundary, and the source of radical ideas may originate from a different country. Therefore, the international partnerships also play a major role in sharing information and developing capabilities.

The counter-radicalization models seem to focus on maintaining freedom of speech and human rights while enforcing a law or government policy. The key features to protect citizens' rights may be discussed in three parts. First, the countries have a well-accepted and well-articulated legal framework. It sets the broad parameters in which the agencies work without impinging human rights. Second, all the government branches – executive, legislative, and judiciary – are involved in their models, and act as watchdogs to one another. Transparency during an investigation remains a key feature of ensuring the rule of law. A single branch cannot enforce a measure without involving others. The LEAs also cannot implement coercive measures without judiciary guidance. For example, the FBI does not abruptly arrest anyone or search his personal properties without

reasonable grounds to suspect or a court warrant.[133] Third, the governments remain answerable to the public primarily through a "free press." Media plays an important role by challenging governments in case of any apparent violation of human rights or infringement of freedom of expression.

Finally, the key elements mentioned above suggest that an integration of constructive and enforcing measures that means "carrot or stick" approaches may lead to successful counter radicalization. There appears to be no one-stop solution to this problem and countries employ a variety of methods in a complementary way. Measures like monitoring, content filtering, reporting, and legal action help to deter the producers of the radical messages. On the other hand, the models also effectively employ constructive measures for developing an enduring social resilience against online radicalization. It includes counter-narratives, community-based interactions, youth development programs, and media engagement. Since radicalization involves psychology, the countries focus on specific cultural contexts while combating radicalization. Particularly the Malaysian and Indonesian approach of "fighting fire with fire" by involving Islamic scholars in developing counter-narratives and social awareness, may be useful for Bangladesh since Muslim population in Bangladesh usually accept the views of Islamic scholars.[134]

[133] FBI, "Frequently Asked Questions," accessed April 18, 2017, https://www.fbi.gov/about/faqs.

[134] Ramakrishna, 212-13.

Analysis of Counter-Radicalization Measures of Bangladesh

This part of the chapter will analyze the effectiveness of Bangladeshi counter radicalization measures. The researcher has identified a few drawbacks of Bangladeshi measures through the literature review. This section of the monograph will examine those in further detail comparing with the successful counter-radicalization models of other countries.

One of the key drawbacks of Bangladeshi measures appears to be its overemphasis on negative measures or hard powers against the spread of radical ideas through the internet by using the stick over the carrot. These measures include content filtering, removing or blocking websites, and legal action which mainly affect the static and publicly accessible websites. They are unable to prevent more dynamic online functions and the "dark webs" that can easily avoid tracking. Therefore, Bangladeshi terrorist groups usually gain access to their target groups by using a broad range of social media, blogs, instant messaging applications, and video sharing sites.[135] Social media like Facebook, Twitter, Reddit, and instant messaging sites are more interactive and effective as a means through which terrorist groups can share their ideologies. Moreover, filtering or removing content from privately owned websites is difficult since such websites rely on user-generated reports, and have their own service user agreements. At times these reports may be misleading as well. Hence, the option of abruptly banning websites may not be a useful tool in a democratic country like Bangladesh.

[135] Sobhan, *The Role of Civil Society in Countering Radicalization in Bangladesh*, 13.

Furthermore, banning websites or social media may not bring the intended result in Bangladesh. A few countries like China, North Korea, and Pakistan have banned social media.[136] Even Bangladesh temporarily blocked Facebook and YouTube in 2015.[137] However, most of the people used proxy servers to bypass the bans, and international communities criticized the government for impinging citizens' access to information. Terrorist groups may also find new ways to circumvent any bans and propagate their messages to their target audiences. In a democratic society, policing people's expression is highly undesirable; thus, the Government of Bangladesh eventually realized that such restriction impeded freedom of expression and lifted the ban.[138] Hence, negative measures are not only challenging but also impracticable.

It has to be kept in mind that fighting extremism online is not analogous to fighting child abuse online.[139] Someone may argue that since child abuse content is filtered from the internet, radical ideas should also be filtered in the same way. Regardless of context, however, any content related to child sexual abuse is immoral and unacceptable to any society. On the other hand, some radical content may not appear

---

[136] Alice Kirkland, "10 Countries where Facebook has been Banned," *Xindex*, February 4, 2014, accessed April 18, 2017, https://www.indexoncensorship.org/2014/02/10-countries-faceboo-banned/.

[137] Sneha Shankar, "Bangladesh Unblocks Facebook After 21 Days; WhatsApp, Viber Restrictions Stay," *International Business Times*, October 12, 2015, accessed November 14, 2016, http://www.ibtimes.com/bangladesh-unblocks-facebook-after-21-days-whatsapp-viber-restrictions-stay-2219519.

[138] Ibid.

[139] Ghaffar Hussain and Dr. Erin Marie Saltman, *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it* (UK: Quilliam Foundation, 2014), 94.

immoral to all societies and can be legal in a variety of contexts such as in an academic forum.[140] It may be possible to express someone's radical viewpoints in many jurisdictions that are not applicable for child abuse. Therefore, lessons learned from fighting against child abuse is not equally applicable for fighting against radicalization.

Negative measures hinder intellectual curiosity and freedom of speech in a progressive democratic society. Radical extremist ideas may generate real intellectual debate that may be even helpful for the society. If government officials and scholars can constructively engage in these debates, it can lead to a greater understanding of the terrorists' activities and their viewpoints.[141] It may also provide insights to implement the counter-radicalization strategy. However, the researcher did not find any evidence that suggests the engagement of the Government of Bangladesh in such intellectual debate.

The literature review suggests that Bangladesh has inadequate sophisticated cyber monitoring and reporting systems. It also appears that the LEAs face challenges to keep pace with the terrorist groups. On the other hand, extremists seem continuously developing technical skills to disseminate their messages despite restrictions. The groups like Jamaat-ul-Mujahideen (JMB) and ABT maintain multiple social accounts in English as well as in native language.[142] Facebook, Twitter, and YouTube have suspended their accounts on numerous occasions. Yet, it is not difficult to create a new account or group under different guises. Most of the time they strongly reemerge to challenge the

---

[140] Ibid.

[141] Ibid., 94-95.

[142] Sobhan, *The Role of Civil Society in Countering Radicalization in Bangladesh*, 11-12.

government by presenting an "accurate" current state of their activities. Moreover, the terrorist groups use social networking sites and exploit the features of the sites in a variety of ways.[143] Since the country has no effective reporting system like the FBI, knowledge of how the online platforms have been used only comes to light after an incident. Identifying and removing a particular content or blocking a secret group on social media is troublesome. It may be possible to remove the extremist content by shutting down the entire platform. However, it is a drastic and unwanted measure. Thus, the Government of Bangladesh may try to monitor and filter static websites, but the dynamic websites are difficult to control.

The government should involve people from all tiers of the country to prevent radicalization since it is a social problem. Except a few fragmented efforts, Bangladesh has not yet developed any well-organized programs to integrate people and promote awareness to potential online threats.[144] Most of the programs are limited to within academic forums, and their effectiveness may be questionable due to lack of proper circulation.[145] The FBI experience, as discussed in chapter 2, reveals that community-based programs are quite effective in promoting public awareness. Furthermore, most of the online platforms and service providers are private in Bangladesh. As such, it is imperative to work with the private sector in order to prevent radicalization. However, the country has not yet developed an effective public-private partnership strategy to

[143] Ibid., 13.

[144] Karim and Balaji, 12-13.

[145] Islam, 165.

empower local communities and private stakeholders.[146] The potential of media in developing general awareness seem to remain overlooked.

The absence of an apex coordinating agency seems to be another major weakness in Bangladeshi counter-radicalization efforts. Its absence may have multi-layered effects. First, there may be a lack of systematic analysis of potential cyber threats. Second, it may be problematic for the government to translate the laws into clear cut executive policies for different agencies involved in countering radicalization. Third, the multiple counter-terrorism agencies working under various ministries lack coordination.[147] There are a few routine interagency meetings at the higher levels. However, due to the dynamic nature of online platforms, continuous and intimate interaction is essential among the agencies. Fourth, capacity building and training of the agencies may not be well coordinated. Therefore, the absence of a unified coordinating agency like the NCTC is one of the fundamental shortcomings of Bangladeshi efforts.

Bangladesh also lacks cyber-related intelligence collection and database management capacity.[148] The country has neither a specific agency to deal exclusively with cyber-related issues nor a central database. The experience of the NCTC shows that a central database with shared access by all related agencies is a prerequisite for successful counter-radicalization effort. Different agencies maintaining their own databases, leads towards a disjointed effort.

---

[146] Ibid.

[147] Ibid.

[148] Ibid., 165-166.

Furthermore, the researcher suggests that Bangladeshi intelligence organizations do not exploit the online platforms for information gathering. The visible presence of online communities that are sympathetic to radical ideas can be a good source of information. The intelligence organizations may extract valuable information from chat rooms and blogs about terrorist activities and their ideologies. Moreover, these websites give an opportunity to engage with the terrorists and their sympathizers in a constructive manner. Active engagement and challenging extremist content online may offer an alternative to the negative measures. The opportunities to defeat the extremists online by positive engagement are now greater than they ever have been since terrorists are increasingly using social and interactive media platforms. However, Bangladesh might not have explored these opportunities.

The legislation enacted by the Government of Bangladesh seem incomprehensive to prevent radicalization in the country. So far, the country has not defined what constitutes "cybercrime."[149] It also solely depends on the existing LEAs to implement the laws. However, at times it may be difficult for them to investigate the issues due to the precise technical nature of cyberspace. A few sections of the laws are criticized for violating freedom of speech and can be used in ambiguous ways.[150] The loopholes in the laws may contribute to ambiguity during legal actions, and impinge citizens' freedom of speech.

---

[149] Murshed, 33.

[150] Committee to Protect Journalists, "Proposed Cyber-Security Bill Threatens Media Freedom in Bangladesh," August 24, 2016, accessed March 6, 2017, https://cpj.org/2016/08/proposed-cyber-security-bill-threatens-media-freed.php.

Lack of an effective counter-messaging strategy is another notable drawback in Bangladeshi mechanisms. Preparation of counter-narratives considering the cultural context and psychology and its dissemination is required to defeat the extremists' propaganda. The Indonesian experience suggests that the Islamic scholars and media can play important roles in this regard. However, there is no visible initiative from the Government of Bangladesh so far. The country has many revered Islamic scholars who have acceptance in the society but have not been integrated with the counter-messaging efforts.

Finally, the absence of cyber-threat related research centers and international partnership impedes Bangladeshi efforts of combating radicalization. The country has no dedicated cyber research center like the IMPACT to analyze the trends of radicalization and recommend policies to the government. The country lacks strong partnerships with the global and regional cyber security agencies such as Asia-Pacific Computer Emergency Response Team (AP-CERT), OIC-CERT, IMPACT for combating radicalization.[151] Therefore, it faces challenges for intelligence gathering and capability building.

To summarize, this section of analysis compared the Bangladeshi counter-radicalization efforts with other successful models and reveals a number of drawbacks. The limitations are briefly listed below:

1. Overemphasis on negative measures leading to restricting freedom of speech.
2. Inadequate technology for monitoring and reporting cyber incidents.

[151] Islam, 165.

3. The absence of an apex agency to coordinate the multiple LEAs.
4. The country has no central database with the provision of shared access by the LEAs, causing hindrance to information sharing.
5. The LEAs lack cyber specialists to investigate critical cases.
6. The legal frameworks appear to be ambiguous and ineffective.
7. Lack of government initiatives in organizing programs to promote social awareness.
8. Media, Islamic scholars, and local communities are not integrated into the countering radicalization programs.
9. No comprehensive approach to prepare and disseminate effective counter-narratives.
10. No dedicated research center on cybersecurity related issues.
11. Lack of international partnership impeding information sharing and capacity building.

The primary question of this research is – "are the counter-terrorism efforts of Bangladesh effective to prevent online radicalization without impinging the citizen's access to information?" The drawbacks mentioned above suggest that the counter-terrorism efforts of Bangladesh seem ineffective to prevent online radicalization without impinging the citizen's access to information.

A Suggested Anti Cyber Radicalization Model

This part of the chapter proposes a sustainable and effective anti-cyber radicalization strategy for Bangladesh. The Government of Bangladesh should adopt a Rubik's Cube approach i.e. solving all facets of radicalization simultaneously instead of

focusing. As such, Bangladesh needs to integrate constructive and coercive measures seamlessly. The researcher attempts to develop this model in light of the key elements of successful models discussed in the previous section. The strategies will be broadly covered in three categories as discussed earlier: reducing supply, reducing demand, and an organizational approach. A generic action plan is illustrated in figure 4.

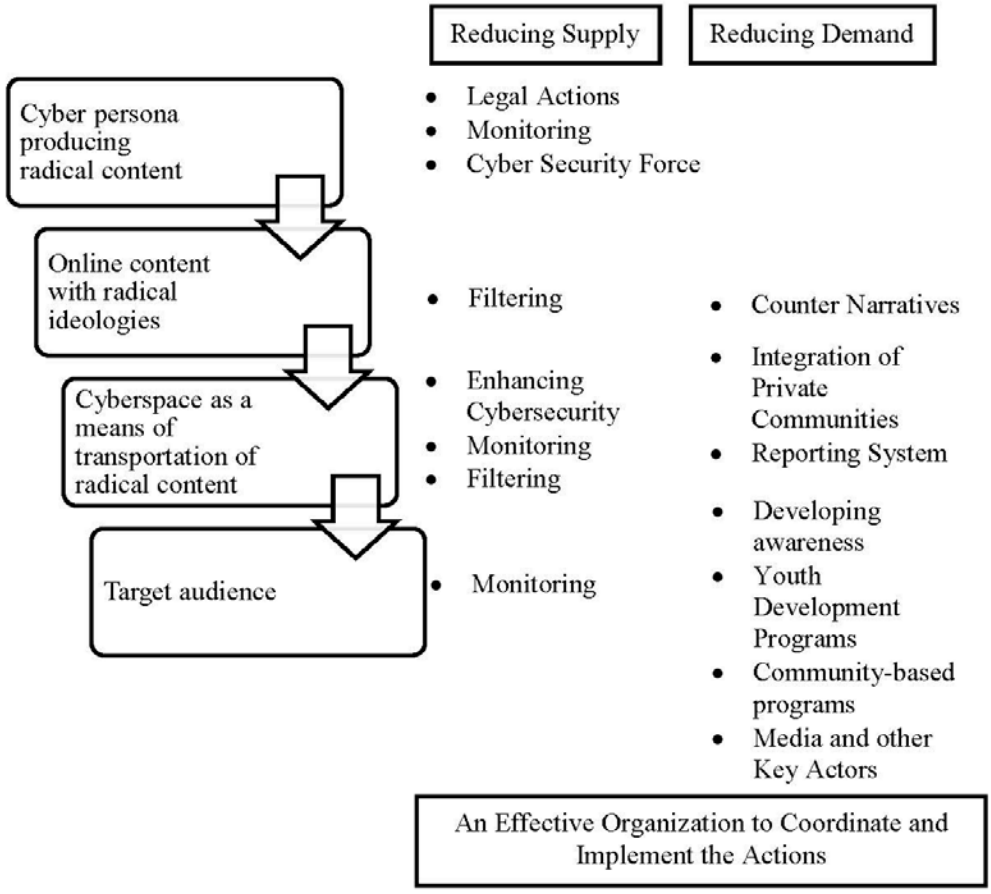

Figure 4. Action Plan to Defeat the Components of Online Radicalization

Source: Researcher's Construct.

Reducing the supply of radical content may be useful for an immediate result, whereas reducing demand for radical content creates an enduring social resilience to radicalization. Hence, the Government of Bangladesh should endeavor to integrate all related stakeholders and emphasize reducing demands to derive long-term benefits. An overarching organization – National Cybersecurity Council – should be formed that will work against radicalization beside cybersecurity issues, and coordinate all related actions by various stakeholders.

Reducing Supply of Radical Content on the Internet

The Government of Bangladesh should reduce the supply of radical content for short-term effects. There are extremists with different levels of motivation, and some are hardcore extremists. As such, the government will have to adopt harsher measures against them. It may be effective, at times, to remove or filter online content if the situation demands. However, there should be a clear legal framework, and the government should maintain transparency to the citizens about its activities. These will ensure freedom of speech and democratic rights of the citizens.

In the beginning, Bangladesh should create an effective legal framework for combating online radicalization. The laws should define “cybercrime” in clear terms. The government may enact necessary legislation that will exclusively deal with cyber-related issues. These laws should sufficiently empower the Cyber Tribunal and LEAs to investigate suspicious incidents and take actions. On the other hand, it should not impinge freedom of speech and human rights. The laws should give a broad guidance to the investigating agencies on maintaining transparency during any legal actions.

Removing and altering content or restricting access would have to be subject to oversight and be open to legal challenges.

Moreover, the government should employ cyber experts at different levels to formulate and implement the laws. Cyber experts should suggest the cyber-related laws. The government may create a central expert body that will translate the laws to executable policies. The LEAs should also have cyber experts for investigating specific cyber-related cases. The government should establish a Cyber Forensic Lab taking the example of the FBI to enhance the investigative capabilities. In order to deal with cybercrimes explicitly, the government may form a Cybersecurity Force in future.

Meanwhile, the Government of Bangladesh is already employing different methods such as monitoring, filtering, and removing content to reduce the supply of radical ideas on the internet. However, various examples from all over the world suggest that the terrorist groups rapidly adopt new technologies, and follow innovative ways to disguise their contents on the web. Due to the dynamic nature of the virtual world, the government should continuously assess its effectiveness and upgrade its technologies. Chapter 2 highlights the concept of cyber persona in which a single producer of radical ideas may create multiple cyber persona by operating different online accounts.[152] Therefore, the law enforcement agencies should have sufficient capabilities to monitor the cyber personas. An exclusive cyber monitoring cell may be established under NTMC or any other agency. Besides, the agencies should monitor the suspicious radical idea producers, and the target groups not only in the virtual world but also in the physical

[152] Office of the Joint Staff, JP 3-12 (R) *Cyberspace Operations,* I-3.

world. In this case, provision of interactive and easily accessible complaint centers like the FBI may be useful.[153]

Nonetheless, reducing supply is an undesirable method, and may not bring intended result. For example, China's "Great Firewall," which consists of a highly complex system of formal and informal controls, and maintained at great expenses can barely keep up with removing objectionable content.[154] Moreover, instant messaging, blogging, video sharing, and social networking platforms have made it difficult to remove or restrict particular types of content. Removing content or restricting access may impinge freedom of speech in a democratic society. Excessive control may also generate a negative public perception that the extremists may exploit. Therefore, the government should carefully determine the limit of censorship within a legal framework without shielding the people from information. The government should preserve the authority of banning a website at very high levels and only to be executed by a judicial order. However, if the government envisages a particular threat due to those ideas, it should have the capacity to detect the sources and prosecute them transparently under existing laws.

---

[153] FBI, "Cyber Crime," accessed December 15, 2016, https://www.fbi.gov/investigate/cyber.

[154] In addition to the "Great Firewall"—a nationwide system of network filters that is maintained by tens of thousands of government employees—the Chinese government has imposed draconian sanctions, including prison, on Internet users promoting "harmful" online content. State and local governments all have units responsible for monitoring online content and usage in their areas. Internet companies operating in China are liable for illegal content posted by their customers. See Lacey Alford, *The Great Firewall of China: An Evaluation of Internet Censorship in China* (Dusseldorf: VDM, 2010).

Reducing Demand for Radical Content to the People

Reducing demand includes methods and approaches that do not diminish the supply, but reduce people's desire to access the content. It is a positive method with better and sustainable effectiveness. The Government of Bangladesh needs to focus significant efforts to defeat radical ideas by peaceful means. The government can play a positive role by helping to create awareness, organize relevant non-governmental actors to conduct various programs, and build a capacity of the local communities. The following paragraphs discuss two important aspects of reducing the demand for radical ideas: promoting awareness and adopting a constructive messaging strategy.

Promoting Awareness

One of the keys to developing social resiliency against online threats is to foster awareness among the general people. Though the internet is related to technology, it does not mean that the solution to online threats needs to be technological. The resiliency of the civic society seems to be more effective than the negative measures. The experience of successful countries suggests investing heavily in building social awareness. Civic challenges to violent extremist online propaganda will be effective if communities understand what they should challenge. Self-aware online users will proactively challenge the radical ideas on the internet. The government of Bangladesh, therefore, should promote awareness about online radicalization among parents, teachers, and community leaders, so that they can detect, report, and intervene in the processes of online radicalization.

The government should involve local communities and media for promoting awareness. It may follow the model of the FBI to engage local communities against

online radicalization.[155] Regular interaction, workshops, and CREX may be helpful in this regard. The government of Bangladesh may implement the U.S. NCTC and FBI strategies such as roundtables and town hall meetings with Muslim communities to develop social awareness. These awareness programs may consist of slide shows and several video clips, highlighting the messages and methods that terrorists use to radicalize people both at home and abroad. The local Islamic scholars should be invited to these programs. The government should also exploit the potential power of media to reach out to all segments of society. Public and private sectors may sponsor different interesting programs, advertisement, and documentary against online radicalization. They should prepare and broadcast various programs for different classes and age groups.

Especially, the government should emphasize developing awareness among youths. Public and private organizations may arrange special awareness programs at the academic or community environments for the youths. Such programs should be designed as per specific age group of the youths to make it interesting. The government should also maintain a few interactive websites like the FBI for different segments of the society. All youths should go through these websites at different academic levels. Through media and community-based programs, the government should also urge parents to take an interest in their children's online activities and to be ready to challenge their behaviors.

[155] FBI, "A New Approach to Countering Violent Extremism: Sharing Expertise and Empowering Local Communities," accessed December 21, 2017, https://leb.fbi.gov/2014/october/a-new-approach-to-countering-violent-extremism-sharing-expertise-and-empowering-local-communities.

Adopting a Constructive Messaging Strategy

The Government of Bangladesh should adopt a comprehensive and constructive messaging strategy to reduce the demand for radical ideas. All related agencies should prepare narratives and counter-narratives based on this central constructive theme. The government should guide all related agencies so that activities of the agencies match with the messages. This strategy should be based on the socio-cultural context of the country. Besides, it should devise a mechanism to monitor the vulnerable groups in the society. It should also constructively engage them in dialogues and address their psychological needs.

The government should endeavor to discredit extremists' propaganda by preparing compelling and logical counter-narratives. The idea of counter-messaging is to expose people to messages that are specifically designed to counter the appeal of extremism. These messages should be built within the overall strategy of positive messaging. A group of highly expert people including Islamic scholars, psychologists, social scientists, security analysts, and other relevant actors should work together for developing effective counter-narratives. It should effectively challenge the violent extremists' ideologies.[156] While preparing the counter-narratives, the authors should look into individual and group psychological vulnerabilities to radicalization within the context of Bangladesh. They should have a deeper understanding of the specific psychological vulnerabilities of different target groups susceptible to radicalization in the

[156] "Radicalisation: The Role of the Internet" (A Working Paper of the PPN, Institute for Strategic Dialogue, London, 2011), 9.

country. It will allow them to deconstruct the extremists' messages, and create more appealing counter arguments.

Proper circulation of the counter-narratives is an imperative for combating radicalization. In cyberspace, these messages can be delivered through websites, blogs, videos, Facebook groups, and other types of online media. From experience, governments seem not to be the most effective conveyor of these messages.[157] Thus, it should take a backseat role while focusing on enabling others' actions. Private partners should be integrated for online search engines optimization. Online searches that include words like extremism, jihad, and ISIS should automatically show counter-narratives up front in the form of advertisements and quick answer boxes. The government should exploit various features of the websites like advertisement links and Facebook pages. It should invest in creating counter-radicalization advertisements on social networking sites. These should automatically appear on the news feeds or play before popular videos. Moreover, media - both print and electronic - should play an important role in broadcasting the counter-narratives. The government should integrate various media production companies who can turn a counter-narrative into a more compelling and attractive visual message.

Moreover, Bangladesh may create virtual and physical anti-radicalization forums through public-private partnerships. Ideally, these forums should have representatives from the government as well as private sectors who have an influential presence on the cyber-domain. The representatives should meet regularly to share ideas, and establish

[157] Hussain and Saltman, 117.

channels of communication with the people. These forums will work to disseminate counter-narratives, and generate awareness among the youths.

An Organizational Approach to Implement the Measures

The government being primarily responsible for ensuring cybersecurity must provide the leadership and extend required facilities. Therefore, it needs a dedicated organization to implement the actions discussed in the preceding sections. Though this organization will work for the overall cybersecurity of the country, this research will discuss only the activities related to online radicalization.

Formation of National Cybersecurity Council (NCC)

Under the umbrella of counter-terrorism efforts, the Government of Bangladesh should form National Cybersecurity Council (NCC) as the apex policy making and coordinating agency. It will be comprised of policy makers from all ministries, LEAs, related government agencies, and other key sectors. A suggested structure of this organization is illustrated in figure 5.

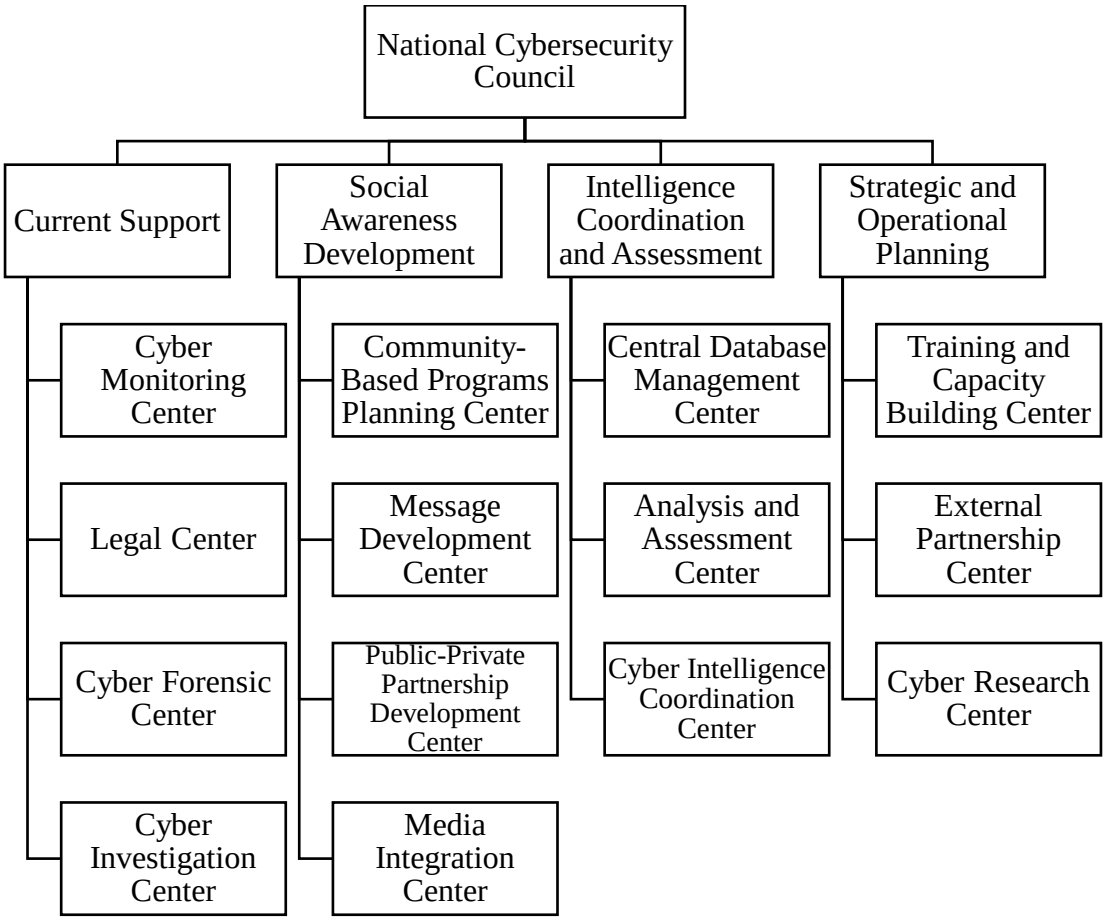

Figure 5. National Cybersecurity Council (NCC)

Source: Researcher's Construct.

The major functions of NCC may include the following:

1. Government policy implementation and oversee the implementation of cybersecurity objectives.
2. Central database management and intelligence coordination.
3. Cyber threat research and risk assessment.
4. Cyber emergency services to include help center, digital forensic center, emergency response team, etcetera.

5. Strategic level interagency cooperation and strategic engagement with global and regional partners like IMPACT, CERT/CIRT, etc.
6. Developing themes for counter-narratives.
7. Training and expertise development.
8. Law and policy suggestion to the government.
9. Private sectors integration.

Current Support: This branch will enhance the security of cyberspace of the country through effective monitoring and proactive action for cyber incident prevention. An overview of the responsibilities of its cells are given below:

1. Cyber Monitoring Center: It will be an exclusive cyber monitoring center to oversee network infrastructure of both private and public entities. This cell will be authorized for online censorship based on judiciary orders or a potential threat.
2. Legal Center: This center will suggest laws and policy related issues to the government. Besides, it will formulate clear-cut policy directives for various agencies of the government in light of laws. This center will strengthen practical collaboration between law enforcement and prosecutorial agencies.
3. Cyber Forensic Center: It will conduct forensic analysis on cyber incidents in coordination with other centers.
4. Cyber Investigation Center: This center will have several investigation-teams, comprised of cyber experts. These teams will deal with specific cases, and provide expert support to the law enforcement agencies.

Social Awareness Development: This branch of the organization will work on developing a sustainable social awareness against radicalization. It will be responsible for coordinating and integrating all government and non-government activities. A few important responsibilities are highlighted below:

1. Community-Based Programs Planning Center: It will plan and coordinate community-based programs to develop awareness including community resiliency exercises and youth development programs. Besides, it will maintain a few interactive websites like the FBI to promote awareness.
2. Message Development Center: This center will develop the overall messaging themes, and provide direction to related actors in developing narratives based on that theme. It will be comprised of different analysts and scholars from different arena to bring different perspectives in the messages. Counter narratives will be embedded within the overall theme.
3. Public-Private Partnership Development Center: It will integrate all related stakeholders of the country, and coordinates a variety of initiatives by public and private sectors. Since most of the internet service providers and cyberspace users are private in Bangladesh, it will be difficult to prevent online radicalization without integrating them. The primary purpose of this center will be to facilitate a platform where all actors can operate cohesively. This center will also manage sponsorships and funding for arranging awareness programs.
4. Media Integration Center: It will integrate all media including print, electronic and social networking sites in the overall counter-radicalization efforts. It will

plan to disseminate the programs mentioned under reducing demand in the previous paragraphs.

Intelligence Coordination and Assessment: This branch of NCC will act as the hub of information and facilitate information sharing among various agencies. It will also provide assessments to the government and other agencies about cyber threats.

1. Central Database Management Center: It will maintain a central database for the country with the provision of shared access by other agencies.
2. Analysis and Assessment Center: This center will provide assessments to the government and law enforcement agencies like the NCTC. This analysis should include all probable websites like social media, blogs, and content sharing sites to mapping the online footprint of suspected organizations and individuals.
3. Cyber Intelligence Coordination Center: Different law enforcement agencies of Bangladesh have a varying degree of cyber intelligence capabilities. Therefore, this center will consolidate their activities under one umbrella. It will assign intelligence collection requirement to the agencies as well as de-conflict intelligence plans.

Strategic and Operational Planning: This branch will be mainly future operations oriented. It will suggest broader issues like international partnership and policy issues to the government. It will also plan and train members of various agencies so that they are prepared to deal with future cyber threats.

1. Training and Capacity Building Center: It will plan and train selected members of various agencies to develop cyber expertise for future. It will also plan and suggest the government for capacity building against radicalization.
2. External Partnership Center: This center will be the government's interface to collaborate with international organizations. The partnerships may include intelligence sharing, technical and procedural assistance and long-term capacity building.
3. Cyber Research Center: The research and development center will continue analyzing the evolving trend of cyber radicalization to develop an appropriate counter mechanism.

Summary of the Interviews

The researcher interviewed two key respondents – Lieutenant Colonel Brian L. Steed, U.S. Army, and Dr. Aleksandra Nesic. Details of the interviews are given in APPENDIX A. This section summarizes their comments.

The interviewees agree that a government should employ hard and constructive measures in a coordinated manner. It should integrate counter-radicalization measures in the virtual world with the physical world. A country should develop capabilities to operate in a broad spectrum of extremists' radicalization efforts. Steed says that LEAs should be able to work across the spectrum of terrorism. Countries should acquire or develop technologies to deter online radical idea producers. Nesic suggests that governments should build capabilities to monitor the emotional-psychological health of the vulnerable groups. It should also engage those groups in multiple ways so that they do

not fall in the prey of extremists. Public and private sectors should engage the vulnerable groups in constructive dialogues and address their psycho-social needs.

Both Steed and Nesic underscored the importance of positive messaging by the government. It should constructively and proactively engage all segments of the society. It should create narratives based on socio-cultural themes instead of merely countering the extremists' narratives. The positive messages should continuously promote inter-faith respect and communal harmony. Some programs and narratives may have a specific target audience while others should attract multiple audiences. The government should take actions that supplement its messages like observance of inter-faith holidays and arranging cross-cultural programs. Besides, counter-narratives should be embedded within the context of the overall constructive messaging theme. All narratives and counter-narratives should be based on socio-cultural context.

Maintaining transparency is one of the key elements while balancing between preventing online radicalization and freedom of expression. However, Steed emphasizes developing ethics and responsibilities of the internet users. He states that responsible online users will create a self-monitoring system that will reduce the need for the government's interference. On the other hand, Nesic highlights the importance of monitoring and filtering by the government while maintaining transparency. The government should create close ties with private actors since they maintain the majority of online platforms. She suggests that public and private stakeholders should create various websites, blogs, and forums to engage different segments of the society constructively.

Summary of Chapter 4

This chapter has evaluated the effectiveness of Bangladeshi measures to counter online radicalization. Initially, it analyzed the significant elements of counter-radicalization model of other countries discussed in chapter 2 that include FBI and NCTC of the USA, and Indonesian and Malaysian efforts. It provided a broad framework about what a country should have to prevent radicalization while maintaining democratic rights of the citizens successfully. Then, it evaluated the Bangladeshi measures in comparison to those elements and unveiled a number of drawbacks. Therefore, the researcher inferred that the counter-terrorism efforts of Bangladesh seem ineffective to prevent online radicalization without impinging the citizen's access to information. It answered the primary question of this research. Finally, this chapter suggested a few measures to the Government of Bangladesh in light of the successful elements discussed previously.

Moreover, the researcher interviewed two key respondents that added valuable insights. Both of them suggest that actions for countering online radicalization should be tied to overall counter-terrorism efforts of a country. The government should take actions in physical world and cyberspace simultaneously. It should also take a "carrot and stick" approach integrating hard and constructive measures. The respondents also emphasized the constructive steps such as psychological engagement with vulnerable groups, positive messaging, and promoting interfaith respect. Besides, they underscored the importance of maintaining transparency by the government about their actions to uphold democratic rights of the citizens.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Cyberspace and the digital domain are growing at an enormous pace. The advent of newer technology, the proliferation of ICT infrastructure, and internet applications have impacted positively on our lifestyle. On the other hand, misuse of these technologies can create serious challenges for global and national security. Digital connectivity has offered us an environment where no country is immune from this threat. As demonstrated in the literature review, the internet has emerged as a new medium for radicalization and recruitment by terrorist groups. It has enabled terrorists to transcend geographical borders and reach any audience anywhere in the world. Many compelling examples across the globe manifest that radicalization through cyberspace is not merely conceptual, rather it is an emerging phenomenon. Bangladesh is also facing this challenge, considering the expanding internet penetration of the country. Various terrorist groups are exploiting the features of online content in innovative ways to spread their ideologies.

The internet has increased opportunities for terrorists to radicalize and recruit people. The concept of territoriality for statehood has become obsolete when it comes to the cyber domain, and extremists can exploit it in a number of ways to spread their propaganda. Many scholars have identified the internet as an accelerant for radicalization. It enables the terrorists to radicalize people, even without personal contact. Using the internet, terrorists can reach out to the vulnerable population to preach their ideologies. Terrorists can also easily conceal their identity in the cyber domain and evade LEAs. The Moghaddam Staircase to Radicalization (figure 1) describes how an individual or a group

of vulnerable people gradually become radicalized. Moreover, the internet has created the opportunity for self-radicalization, given the abundance of radical content available openly on the internet. Therefore, the internet is becoming a useful tool for terrorists to engage with large audiences and implant their beliefs in people's mind.

The terrorists adopt a wide variety of techniques to exploit the online platforms. Sometimes they create dedicated websites and skillfully conceal them from government monitoring. They also follow different techniques such as dead drops and paraciting while spreading radical content. Of particular note, social media like Facebook and Twitter have numerous features that the terrorists are adeptly exploiting. Social media provides an easy way to reach more people because of its large number of users and broad appeal. Anyone can create a secret or closed group and add people to that group where he can start posting radical content. Extremists can anonymously continue their online activities using social media sites. It is extremely difficult to identify such accounts and groups unless someone reports with evidence. Furthermore, it is very easy to create a new account or group if a LEA takes down an account. Hence, terrorists may either create their own websites or use existing online platforms to disseminate their radical messaging.

Online radicalization may emerge as an even more serious security concern for Bangladesh in the near future. The government of Bangladesh has assigned priority to the digitization of various sectors, and the numbers of internet users are steadily increasing in the country. This increased number of the web users has created more chances for online radicalization. A few homegrown terrorist organizations such as JMB and ABT are already maneuvering in cyberspace. These groups are gradually developing their

technical expertise and may be able to expand and exploit their online presence in the absence of government action. These groups may maintain some clandestine connections with global terrorist organizations like ISIS and Al Qaeda and may be able to acquire sophisticated technical skills from them. Though there is no convincing evidence of their physical link with these global terrorist organizations, the possibility of maintaining covert connections in the virtual world cannot be overruled. Their online activities may grow as a threat to the national security of Bangladesh.

Bangladeshi youths are particularly vulnerable to radicalization. The young generation is tech-savvy but may lack cybersecurity awareness. The involvement of young and educated youths in the atrocity at the Holey Artisan Restaurant in Dhaka demonstrated the potential risks of online radicalization. Extremists skillfully exploit the emotion of the Bangladeshi people such as religious sentiment and socio-economic deprivation. Doctored messages and false information on the websites have successfully triggered communal violence on several occasions.

The government of Bangladesh mainly uses hard power against terrorism and radicalization. These measures include direct action against terrorists, monitoring, and filtering online content. It has also blocked a few social media sites in an attempt to prevent potential security threats. However, implementing such coercive measures in a democratic society is neither practicable nor desirable. Impinging freedom of speech and access to information may hinder social and economic development. Therefore, the challenge is to balance these two competing requirements: preventing online radicalization and ensuring a free flow of information. In this context, this research attempted to evaluate the effectiveness of Bangladeshi measures to prevent online

radicalization while ensuring freedom of speech and access to information. The researcher has analyzed a few successful counter radicalization models – the FBI and NCTC of the USA, and the efforts of Indonesia and Malaysia – to determine the key elements of cyber success. This research provided a framework to assess the effectiveness of Bangladeshi measures.

The successful counter radicalization models discussed in chapter 2 highlighted a few key concepts. The models appear to suggest a combination of hard and soft powers may be most effective i.e. adopting a carrot and stick approach. Coercive measures such as monitoring, filtering, and legal action seem to produce only short-term effects. These measures, however, are not desirable in a democratic society.

In contrast, The NCTC in the U.S. coordinate the activities of all related agencies. It maintains a central database and advice policy matters to the government. The United States, Indonesia, and Malaysia also have functional international partnerships for enhancing their own capacity. They invest heavily in developing cybersecurity awareness among the general people and conduct many community-based programs such as Community Resilience Exercise and youth development programs. These programs empower the individual and society to detect and counter the online radical content. Furthermore, countries like Indonesia and Malaysia prepare effective and appealing counter-narratives against extremist propaganda. They integrate Islamic scholars and private sector within the overall approach. Therefore, ideal counter-radicalization programs should integrate the activities of the virtual and physical world simultaneously.

The models discussed above employ various measures while limiting negative effects on citizens' democratic rights and freedom of speech. The legal framework of the

United States, Indonesia, and Malaysia sets the broader parameter for the LEAs activities. For example, the FBI's investigation of Nigerian terrorist Abdulmutallab demonstrates how to effectively maintain transparency and human rights while dealing with terrorism. Besides different branches of the government continuously oversee other's activities. Thus, a comprehensive legal framework and attempt to maintain transparency appear to be the keys to protect citizens' democratic rights.

This research has also identified a few weaknesses in Bangladesh's overall counter-radicalization efforts. First, it mostly employs hard powers in an attempt to prevent radicalization. The government was criticized for shutting down social media sites in the country, and it may not be a practical approach in a democratic society, certainly not in the longer term. Second, a number of LEAs are operating in the country against terrorism, but there is no apex agency to coordinate their efforts. Strategic direction and physical actions are not tied properly due to lack of this agency. Third, the country lacks required technology to monitor and acquire information. There is no central database with shared access facilities by all related agencies, causing a lack of information flow. It also forces the LEAs to remain reactive to terrorist activities rather than proactive. Fourth, Bangladesh lacks functional international partnerships and a dedicated cybersecurity research centers. In an interconnected world, no country can guarantee absolute safety without these relationships and resources. Unfortunately, Bangladesh appears to be reluctant to build partnerships with developed countries. These drawbacks degrade her capacity to counter radicalization.

The Government of Bangladesh also lacks the initiative to develop cybersecurity awareness among the general people. Though the private sector has organized a few

programs on this issue, those are limited to the academic environment. An understanding of cybersecurity is unclear among the general population. The private sector, Islamic scholars, and the media are not well integrated within overall counter-radicalization efforts. There is no visible effort to disseminate positive narratives or at least counter-narratives. Besides, the existing legal provision seems to be inadequate to deal with contemporary cyber threats. The country's legal framework appears to be ambiguous and does not define what constitutes harmful online content. It does not sufficiently empower the Cyber-tribunal for prompt judicial action. Scholars and journalists of the country have criticized a few of the laws that the government or LEAs may use for restricting freedom of expression. Therefore, Bangladesh faces challenges in multiple dimensions to counter online radicalization.

It is challenging for the Government of Bangladesh to safeguard her citizens from cyber threats while keeping the domain open and innovative. The government approach to counter radicalization can be divided into three categories: reducing the supply of radical content, reducing demand for radical ideas, and an organizational approach to implementing the measures. At first and for a short time, in order to reduce the supply of radical messaging existing measures such as monitoring, filtering, and legal actions against the producers of radical content should continue. The country should develop its technical capabilities along with an expert workforce to monitor cyberspace and filter content. In addition, it should develop well-articulated laws and a cybersecurity strategy that will guide such actions while ensuring freedom of speech, opening up access over time and reducing restrictive measures.

On the other hand, the government should underscore positive measures for developing an enduring social resiliency against radicalization. It should develop a mechanism to detect vulnerable individuals or groups and ensure psycho-social engagement with them. A public-private partnership approach may be effective to engage communities and develop cybersecurity awareness. The government should particularly arrange programs for the youth to empower them to detect radical content and take preventive measures. An effort to promote ethical and responsible behavior among online users will create a self-monitoring system in the cyberspace. It will allow the government to protect citizens' freedom of speech by reducing its interference in the cyber domain. In addition, the government should start positive messaging to foster communal harmony. Counter-narratives should be embedded within this overall approach.

Bangladesh needs an effective organization to implement these counter-radicalization strategies. The country should immediately establish the NCC as part of its overall counter-terrorism effort. This apex agency will coordinate all LEAs under a unified umbrella, and act as a link between the government's strategy and stakeholders' actions. It will maintain a central database for rapid information sharing and act as an interface with foreign partners.

Finally, online radicalization is a serious concern not only for Bangladesh but also for global communities. In the present interconnected world, all countries should work in a concerted manner to arrest this menace. With the advent of technologies, terrorists will continue to adopt innovative ways for radicalization and recruitment. Therefore, governments should remain proactive to anticipate future patterns and take appropriate actions in the initial stage. Eliott Abrams, a prominent American diplomat, rightly

pointed out, "*We need to understand that an open society and free speech and press... really are the best weapons against al Qaeda and extremism*."[158] Therefore, the global communities should uphold citizens' freedom of expression and develop a resilient society against radicalization.

Recommendations

Recommendations for the Government of Bangladesh

Based on the findings of this study, the researcher recommends the following to the Government of Bangladesh:

1. Establish a National Cybersecurity Council in order to achieve unified action, an overarching agency to implement government policies.
2. Develop an active messaging strategy to promote communal harmony in the country. Counter-narratives may be embedded within this holistic approach to defeating radical ideas. Private partners may be integrated to prepare and disseminate appealing positive messages.
3. Initiate community-based programs and youth development programs to build an enduring social resiliency against radicalization. The government should develop a strategy to detect vulnerable groups in the country who are susceptible to radicalization and ensure their psycho-social engagement.

[158] Brainy Quote, "Eliott Abrams Quotes- Page 2," access May 5, 2017, https://www.brainyquote.com/quotes/authors/e/elliott_abrams_2.html.

4. Review existing laws and policies related to cybersecurity issues, and formulate laws that sufficiently empower LEAs to act against cyber threats while protecting the citizens' democratic rights.

Recommendation for Future Research

Radicalization through cyberspace will remain a concern for Bangladesh in future. Therefore, more researches from different perspectives are required to understand it and suggest effective counter-measures. This research has set the condition for further in-depth study. For this study, the researcher conducted qualitative analysis and interviewed two scholars only. In future, a combination of qualitative and quantitative analysis may be conducted. Surveys and some interviews of Bangladeshi scholars will bring some additional perspectives. Moreover, researchers may study the measures of other countries that may be effective in the context of Bangladesh

In future researchers may also study how Bangladesh can develop an active messaging strategy to foster communal harmony. It may analyze how the private sector can be integrated with government efforts to achieve a common objective. It should also highlight how the country can monitor the vulnerable groups and constructively engage them to address their psycho-social needs. Counter-narratives should be embedded within the overall strategy. Researchers should examine the messaging strategies of the U.S. in various countries like Iraq and Afghanistan to gain a better understanding. This research may also follow a mixed method analysis, combining qualitative and quantitative analysis.

A study may be carried out to suggest a cybersecurity strategy for Bangladesh. This research may have multiple dimensions. Based on this study, future researchers may

analyze how the country can avert the spread of radical content through the cyber domain. It should suggest possible ways to prevent exploiting social media sites by the extremists. Researchers may obtain expert opinions directly from the social media companies since many of them are based in the United States.

APPENDIX A

SUMMARY OF INTERVIEW

Survey Protocol Approval Number: 17-04-001

Lieutenant Colonel Brian L. Steed, US Army

Lieutenant Colonel Steed is currently an assistant professor of Military History at the US Army Command and General Staff College and a Middle East Foreign Area Officer. He served eight and a half consecutive years in the Middle East including assignments in the Levant, Mesopotamia, and the Arabian Peninsula, giving him an immersed perspective in terrorism in the contemporary world. He has written numerous books and articles on various issues of terrorism like *ISIS: An Introduction and Guide to the Islamic State*, *Voices of the Iraq War: Contemporary Accounts of Daily Life (Voices of an Era),* and *Maneuver in the Narrative Space.*

Question: What do you believe are the broad capabilities a country needs to develop for countering radicalization through cyberspace?

Answer: The spectrum of radicalization and recruitment is vast. Extremists may employ a combination of different methods like personal motivation and virtual contact to radicalize people. Thus, a country should develop its capabilities encompassing the broad spectrum of extremists' radicalization efforts. Countering online radicalization should be coordinated with the overall counter-terrorism efforts of a country. It should include hard measures like direct action against the extremists, online monitoring, filtering as well as constructive measures such as developing social awareness. LEAs should be able to work across the spectrum of terrorism. Countries should acquire or

develop technologies to deter online radical idea producers.

Question: It is challenging to find the balance between preventing online radicalization while ensuring the free flow of information. How can a nation best balance these two requirements?

Answer: Developing responsibility and ethics of the online users may facilitate a nation to balance the two conflicting requirements. If the online users are responsible, they can impose a self-monitoring system in that marketplace. The awareness and ethical development should start from the young ages. It will be a lot easier for them to identify an irresponsible behavior in cyberspace such as spreading radical ideas, and they will stand against those ideas. Eventually, it will allow free flow of information while defeating the radical ideas by the online users, reducing government interference.

Question: Positive measures against online radicalization like developing social awareness and counter-narratives seem effective and sustainable. Are there other positive measures you believe a country should adopt in the short and long term?

Answer: The government should create a positive and engaging messaging strategy instead of merely countering the extremists' narratives. For example, during a war a force does not prepare the counter bombardment plan only; it creates an overall offensive or defensive fire plan, and counter bombardment plan fits within that. Likewise, while maneuvering in the narrative space, it should have an overall plan to defeat the extremists' ideologies comprehensively. The government plan should include preparation and dissemination of constructive messages to the people like the positive aspects of religions, interfaith respect, and communal harmony. Some programs and narratives may

have a specific target audience while others should attract multiple audiences. Counter-narratives should work within this overall plan to defeat the arguments of the extremists. Besides, governments should promote inter-religion respects by different programs such as inter-faith holidays.

Question: What sort of broad legal frameworks do you suggest or know about that sufficiently empower law enforcement agencies, while ensuring transparency in their investigation?

Answer: The legal framework should guide the government to communicate with the people about its activities against radicalization continuously. If people understand the government's intent, the majority of them reasonably accept its activities. In a democratic society, people become skeptic while they remain unaware of the government's action. Therefore, the legal frameworks should guide the branches of the government to oversee each other, and remain open to the people. It should also allow judiciary challenge to any government action.

Dr. Aleksandra Nesic

Dr. Aleksandra Nesic is a Research & Teaching Professor of Cultural-Conflict Psychology at US Army John F. Kennedy Special Warfare Center and School (USASOC/SOCOM) and a Visiting Teaching Professor, Combatting Terrorism Fellowship Program at Joint Special Operations University, MacDill AFB, USSOCOM. Her research areas include political violence, revolutionary social movements, psycho-cultural and ethnic identity conflicts, and state building. The opinions of an active duty military and an academician add greater depth to this study.

Question: What do you believe are the broad capabilities a country needs to develop for countering radicalization through cyberspace?

Answer: A country should be able to implement multiple measures not only in cyberspace but also in social communities to prevent radicalization. In the society there are individuals as well as group of people who suffer from insecurity, trauma, or sense of deprivation. Extremists groups usually appeal to the emotional aspect of these vulnerable people. For example, the mass refugees across the world who are traumatized, searching for a shelter, and deprived of psycho-social health can be easily victimized by the appealing messages of the extremists. Thus, the government should monitor the emotional psychological health of the people, build capabilities - on ground and in cyberspace – to detect vulnerabilities of marginalized or traumatized people, and develop a strategy to build resilience among those individuals or groups. Government should build psychological engagement capabilities with the vulnerable groups so that they do not fall in the prey of extremists.

Question: It is challenging to find the balance between preventing online radicalization while ensuring the free flow of information. How can a nation best balance these two requirements?

Answer: It is becoming increasingly challenging due to the spread of the internet and spirit of democracy. The government filtering of online content should continue if it identifies something as potentially harmful. However, it does not mean a “blank check” to the government to take down any online content. It should take down those content only that have been confirmed as harmful. The government should maintain closer ties and transparency with private organizations who maintain the online platforms. The

Government should set a framework to define what constitutes dangerous online content. Besides, it should endeavor to create social media accounts, blogs, and various websites that will empower the people to identify the radical ideas. Overall, whatever the government does, it should remain open to the citizens.

Question: Positive measures against online radicalization like developing social awareness and counter-narratives seem effective and sustainable. Are there other positive measures you believe a country should adopt in the short and long term?

Answer: Positive messaging can be an effective way to fight radicalization. Counter-messages should be developed based on cultural context. For example, the counter-messages against ISIS, Al Qaeda, and Boko Haram are very American or Western-centric. It may not be appealing to the people of middle-eastern countries. Thus, messaging strategy should address the cultural aspects particular to that country. The government should understand the psycho-social requirement of the vulnerable groups, and adopt strategies to build resiliency among them. Moreover, it should continuously highlight the ongoing positive images related to religions, ethnicities, or societies.

BIBLIOGRAPHY

Books

Alarid, Maeghin. *Impunity: Countering Illicit Power in War and Transition*. Edited by Michelle Hughes and Michael Miklaucic. Washington, DC: National Defense University, 2016.

Behr, Ines V., Anaïs Reding, Charlie Edwards, and Luke Gribbon. *Radicalisation in the Digital Era*. United Kingdom: RAND Corporation, 2103.

Bjelopera, Jerome P. *American Jihadist Terrorism: Combating a Complex Threat*. Washington, DC: Congress Research Service, 2011.

Hussain, Ghaffar, and Dr. Erin M. Saltman. *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It.* UK: Quilliam Foundation, 2014.

Pantucci, Raffaello. *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists*. London: International Centre for the Study of Radicalisation and Political Violence, 2011.

Powers, Shawn, and Matt Armstrong. *Visual Propaganda and Extremism in the Online Environment*. Edited by Carol K. Winkler and Cori E. Dauber. Carlisle, PA: The United States Army War College Press, 2014.

Precht, Tomas. *Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism*. Copenhagen: Danish Ministry of Defence, 2008.

Sobhan, Farooq. *The Role of Education in Countering Radicalization in Bangladesh*. Dhaka: Bangladesh Enterprise Institute, 2015.

Stern, Jessica. *Terror in the Name of God: Why Religious Militants Kill*. New York: Harper Perennial, 2003.

Weimann, Gabriel. *New Terriorism and New Media*. Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014.

———. *Terror on the Internet: The New Arena, The New Challenges*. Washington, DC: United States Institute of Peace Press, 2006.

Wilner, Alex S., and Claire-Jehanne Dubouloz. *Homegrown Terrorism and Transformative Learning: An Interdisciplinary Approach to Understanding Radicalization.* Taylor and Francis Online: Global Change, Peace, and Security 22:1, 2010.

Yeap, Su Y., and Jenna Park. *Countering Internet Radicalisation: A Holistic Approach.* Singapore: S. Rajaratnam School of International Studies, 2010.

Periodicals

Islam, Aynul M. "Mapping Terrorism Threats in Bangladesh." *Bangladesh Institute of International and Strategic Studies* 29, no. 2 (April 2008): 153-176.

Khan, Shahab E. "Bangladesh: The Changing Dynamics of Violent Extremism and the Response of the State." *Small Wars and Insurgencies* 28, no. 1 (2017): 191-217.

Moghaddam, Fathali M. "The Staircase to Terrorism, A Psychological Exploration." *American Psychologist* 60, no. 2 (2005): 161-169.

Murshed, Mahboob. "A Comparative Analysis between Bangladeshi and Korean Legal Frameworks for Combating Cybercrime to Ensure Cyber Security." *Korean University Law Review* 19, no. 23 (2016): 23-40.

Neumann, Peter R. "Options and Strategies for Countering Online Radicalization in the United States." *Studies in Conflict and Terrorism* (2013): 431-459.

Ramakrishna, Kumar. "The Southeast Asian Approach to Counter-Terrorism: Learning from Indonesia and Malaysia." *The Journal of Conflict Studies* (Summer 2005): 27-47.

Schmidle, Robert E. "Positioning Theory and Terrorist Networks." *Journal for the Theory of Social Behaviour* 40, no. 1 (2010): 65-78.

Government Documents

Office of the Joint Staff. Joint Publication 3-12 (R), *Cyberspace Operations*. Washington, DC: Government Printing Office, 2013.

———. Joint Publication (JP) 3-13, *Information Operations*. Washington, DC: Government Printing Office, 2012.

The White House. *National Security Strategy 2010*. The White House, Washington, DC, 2010.

U.S. Department of Justice. *Online Radicalization to Violent Extremism.* Washington, DC: Department of Justice, 2014.

Internet Articles

Arman, Tanbir U. “New Media, Digital Radicalization and Social Security.” *The Bangladesh Today*, September 8, 2015. Accessed November 14, 2016. http://thebangladeshtoday.com/2015/09/new-media-digital-radicalization-and-social-security/.

Bashar, Iftekharul. “Violent Radicalisation in Bangladesh: A second wave?” *The Nation*, 2013. Accessed December 18. 2017. http://www.nationmultimedia.com/news/opinion/aec/30217330.

Byron, Rejaul K. “Bangladesh to Purchase Modern Surveillance Equipment.” *The Daily Star*, August 3, 2015. Accessed March 14, 2017. http://www.thedailystar.net/frontpage/govt-buy-new-surveillance-tools-120967.

Committee to Protect Journalists. “Bangladesh.” CPJ.org, August 24, 2016. Accessed March 6, 2017. https://cpj.org/2016/08/proposed-cyber-security-bill-threatens-media-freed.php.

Facebook. “Information for Law Enforcement Authorities.” Facebook.com. Accessed November 1, 2016. https://www.facebook/com/safety/ groups/law/guidelines.

FBI. “Cyber Crime.” Accessed December 15, 2016. https://www.fbi.gov/investigate/cyber

Ferdinando, Lisa. “Unprecedented Challenge in Countering Adversarial Propaganda.” *DoD News*, October 23, 2015, Accessed November 1, 2016. http://www.defense.gov/News-Article-View/Article/625750/unprecedented-challenge-in-countering-adversarial-propoganda-official-says.

Ghosh, Nirmal. “Battle for Bangladesh's Soul as Islamic Radicals Push for Power.” *The Strait Times*, August 2, 2016. Accessed February 21, 2107. http://www.straitstimes.com/opinion/battle-for-bangladeshs-soul-as-islamic-radicals-push-for-power.

Hardy, Roger. “Thailand: The Riddle of the South.” *BBC News (UK Edition)*, 15 February 2005. Accessed December 18, 2017. http://66.102.7.104/search?q=cache:d6gWMF8Gez4J:news.bbc.co.uk/1/hi/world/asia-pacific/4264195.stm+kru+se+mosque,+thailand&hl=en&ie=UTF-8.

Hasan, Kamrul. “82% Bangladeshi Militants Radicalised Through Social Media.” *Prothom Alo*, March 24, 2017. Accessed April 3, 2017. http://en.prothomalo.com/bangladesh/news/143243/82%25-Bangladeshi-militants-radicalised-through.

Internet World Stats. “Asia Internet Use, Population Data and Facebook Statistics - March 2017.” Internet Coaching Library. Accessed November 15, 2016. http://www.internetworldstats.com/stats3.htm#asia.

Manik, Julfikar A., and Ellen Barry. “Hindu Temples and Homes in Bangladesh Are Attacked by Muslim Crowds.” *The New York Times*, November 2, 2016. Accessed March 4, 2017. https://www.nytimes.com/2016/11/03/world/asia/hindu-muslim-bangladesh.html.

Manik, Julfikar A., and Geeta Anand. “After Slaughter, Bangladesh Reels at Revelations About Attackers.” *The New York Times*, July 3, 2016. Accessed March 14, 2017. https://www.nytimes.com/2016/07/04/world/asia/bangladesh-dhaka-terrorism.html.

Markar, Marwaan M. “Push Muslims Too Hard and Risk Jihad.” *Asia Times*, 26 February 2005. Accessed January 12, 2017. http://66.102.7.104/search?q=cache:dY0M0hzVWdEJ:www.atimes.com/atimes/Southeast_Asia/GB26Ae03.html+kru+se+mosque,+thailand&hl=en&ie=UTF-8.

Population Reference Bureau. “Bangladesh.” Prb.org. Accessed November 10, 2016. http://www.prb.org/DataFinder/Geography/Data.aspx?loc=378.

Price, Matthew. “Anders Breivik describes Norway Island Massacre.” *BBC*, April 20, 2012. Accessed November 11, 2016. http://www.bbc.com/news/world-europe-17789206.

Shane, Scott. “Inside Al Qaeda’s Plot to Blow Up an American Airliner.” *The New York Times*, February 22, 2017. Accessed March 5, 2017. https://www.nytimes.com/2017/02/22/us/politics/anwar-awlaki-underwear-bomber-abdulmutallab.html.

Shankar, Sneha. “Bangladesh Unblocks Facebook After 21 Days; WhatsApp, Viber Restrictions Stay.” *International Business Times*, October 12, 2015. Accessed November 14, 2016. http://www.ibtimes.com/bangladesh-unblocks-facebook-after-21-days-whatsapp-viber-restrictions-stay-2219519.

Statistics Brain Research Institute. “Facebook Company Statistics.” Static Brain. Accessed November 1, 2016. http://www.statisticbrain.com/facebook-statistics/.

Summers, Chris. “Pictured: The Grinning ISIS Terrorists who Hacked 20 Innocent Victims Including Westerners to Death but Spared those who could Recite the Koran in Bangladesh Attack.” *The Daily Mail*, July 2, 2016. Accessed March 14, 2017. http://www.dailymail.co.uk/news/article-3671586/Pictured-grinning-ISIS-terrorists-hacked-20-innocent-victims-including-westerners-death-spared-recite-Koran-Bangladesh-attack.html.

Terrorism Research and Analysis Consortium. “Ansarullah Bangla Team (ABT).” Accessed March 4, 2017. https://www.trackingterrorism.org/group/ansarullah-bangla-team-abt.

The Indian Express. "List of Recent Attacks in Bangladesh Blamed on Radical Islamists." July 2, 2016. Accessed November 14, 2016. http://indianexpress.com/article/world/world-news/list-of-recent-attacks-in-bangladesh-blamed-on-radical-islamists-2888881/.

Travis, Alan. "Internet Biggest Breeding Ground for Violent Extremism." *The Guardian*, February 5, 2012. Accessed December 17, 2016. https://www.theguardian.com/uk/2012/feb/06/internet-violent-extremism-breeding-ground.

Twitter. "It's What Happening." Accessed November 1, 2016. https://about.twitter.com/company.

UN E-government Knowledge Database. "Bangladesh." Accessed January 21, 2017. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/14-Bangladesh.

YouTube. "Statistics." YouTube 2016. Accessed November 1, 2016. https://www.youtube.com/yt/press/statistics.html.

Other Sources

Bergin, Anthony, Sulastri B. Osman, Carl Ungerer, and Nur A. Mohamad Yasin. "Countering Internet Radicalisation in Southeast Asia." Special Report, Issue 22. Canberra: Australian Strategic Policy Institute, 2009.

Briggs, Rachel, and Alex Strugnell. "Radicalisation: The Role of the Internet." Policy Planners' Network Working Paper, Institute for Strategic Dialogue, London, 2011.

Holmer, Georgia. "Countering Violent Extremism: A Peace building Perspective." Special Report 336, United States Institute of Peace, Washington, DC, 2013.

International Multilateral Partnership against Cyber Threats. "Impact." Presentation. Accessed November 15, 2016. http://www.itu.int/ITU-D/conferences/rpm/2009/asp/documents/IMPACTOverview.pdf.

Karim, Tariq, and Dr. Balaji Madhumita S. "Rising Trend of Religious Radicalization in Bangladesh." Issue Brief, Vivekananda International Foundation, New Delhi, 2016.

Ministry of Home Affairs. "The Jemaah Islamiyah Arrests and the Threat of Terrorism." White Paper, Ministry of Home Affairs, Singapore, January 7, 2003.

Neumann, Peter R. "Countering Online Radicalization in America." Homeland Security Project Report, Bipartisan Policy Center, Washington, DC, December 2012.

Reinwald, Brian R. “Assessing the National Counterterrorism Center’s Effectiveness in the Global war on Terror.” Research, US Army War College, Carlisle, PA, 2007.

Silber, Mitchell D., and Arvin Bhatt. “Radicalization in the West: The Homegrown Threat.” Report, New York City Police Department, New York, 2007.

Technical Analysis Group. “Examining the Cyber Capabilities of Islamic Terrorist Groups.” Research, Dartmouth College, New Hampshire, 2003. Accessed: January 21, 2017. www.ists.dartmouth.edu/library/164.pdf.

Torok, Robyn. “Make a Bomb in Your Mums Kitchen: Cyber Recruiting and Socialisation of White Moors and Home Grown Jihadists.” Conference Proceeding, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2010.