BIISS JOURNAL, VOL. 39, NO. 2, APRIL 2018: 215-234 biiss journal

Md. Jahan Shoieb

ROLE OF INTERNET-BASED ALTERNATIVE MEDIA IN GLOBAL TERRORISM AND COUNTERTERRORISM

Abstract

Global terrorism is a multi-dimensional concern. Nowadays, terrorists use multifaceted tactics in order to avoid various counterterrorism operations. In recent years, a comprehensive drone campaign by the United States and death of some top leaders pushed Al Qaeda, Islamic State and other terrorist groups to find out alternative ways to convey their messages to their followers and sympathizers. Terrorist groups are resorting to internet-based alternative media to spread terrorism. Internet is also helping terrorist groups in training, fundraising, recruiting manpower, planning and executing terrorist attacks. Lone-wolf terrorists are also taking advantage of internet-based media in communication technologies. Internet has brought a shift in the spectra of global terrorism. An understanding of the linkage between terrorism and internet-based alternative media can help in formulating a counterterrorism strategy. This paper examines the role of the internet-based alternative media in global terrorism and counterterrorism. The research finding suggests that terrorist groups are quite successful in using internet-based alternative media to reach their audiences. It is also evident that the internet also can play an important role in global counterterrorism efforts.

Keywords: Alternative Media, Internet, Terrorist group, Terrorism, Counterterrorism

1. Introduction

Modern communication technology has profound impacts on every aspect of daily life. Global terrorism has also manipulated the advantages of the modern communication system, which helped terrorist groups reach their audiences independently bypassing the mainstream mass media. In fact, one of the pressing challenges for the global community is the use of internet-based alternative media by terrorists to inspire, incite and direct their followers and sympathizers. History suggests that previously terrorists faced difficulty to spread their messages and, therefore, their scope was limited. There are two main reasons behind this. Firstly, they had no control over whether their images of violence and messages of terrorism would be covered by news media in real time. Secondly, they could not control the two-step process of mediated communication. Thus, there was no guarantee that the mainstream media would cover their news. Even if any media covered their story, editor of the respective media would choose the angle by which the news was presented to the audience.[1]

Md. Jahan Shoieb is Research Fellow at Bangladesh Institute of International and Strategic Studies (BIISS). His e-mail address is: jshoieb@gmail.com

[1] Bruce Klopfenstein, "Terrorism and the Exploitation of New Media", in Anandam P. Kavoori and Todd Fraley

For a better discussion, it is important to distinguish mainstream and alternative media. Generally, commercial or mainstream media are controlled, operated and funded through large conglomerate businesses. This characteristic is absent in the case of alternative media. They are primarily funded through donations of different kinds. While differentiating the two terms, most of the literature suggest that alternative media outlets function without the influence of corporate power and work as resistant to the conventional media outlets and their perspectives.[2] There are different uses of the term alternative media ranging from community radio to an organization's own website. Probably the most popular definition of alternative media is all media which are somehow opposed to or have tension with mainstream media.[3] In recent times, the use of internet has complicated the difference between mass and alternative media. However, the use of internet has opened a vast arena for alternative media channels. A classic example of this can be found in Indymedia.org, an internet-based media found during 1999 World Trade Organization (WTO) protests in Seattle. Notably, the Indymedia allows anyone to upload news content of different types (photos, print, audio or video) to the website. With the explosion of the blogosphere, this kind of 'do it yourself' (diy) media is increasing rapidly.[4] In this article, mainly, the internet-based media is considered as alternative media, which also includes terrorist groups' own websites. And the internet means all communication, content or activity which takes place in the world wide web (www).

In the past, reliance on mass media for disseminating terrorist ideology to mass people and terrorists' sympathizers was one of the key features of global terrorism. In fact, some people still believe that there is an intrinsic relationship between terrorism and mass media. Apparently, without media's involvement, the impact of terrorism is wasted, remaining narrowly to the immediate victims rather than reaching a wider target audience at whom the terrorist group's violent act is aimed.[5] Thus, most of the terrorist groups previously used media as a part of their tactics. Terrorist groups needed the help of the media, and media, on the contrary, had to rely heavily on them to get sensational news for boosting up their Target Rating Point (TRP). Terrorist groups sought publicity for their acts and they believed that mass media can quickly spread their news and views to a wide range of audience, which they could not do by themselves. However, heavy reliance on mass media started to decline with the invention of the internet and more specifically with the wide expansion of internet-based social networking websites.

(eds.), *Media, Terrorism, and Theory,* Maryland, USA: Rowman & Littlefield Publishers, Inc., 2006, p. 108.

[2] Michael Kenny, "Beyond the Internet: Mtis, Techne, and the Limitations of Online Artifacts for Islamist Terrorist", *Terrorism and Political Violence*, Vol. 22, No.2, 2010, pp. 204-222.

[3] Victor W. Pickard, In Todd M. Schaefer and Thomas A. Birkland (eds.), *The Encyclopedia of Media and Politics*, Washington, DC: CQ Press, 2007, pp. 12-13.

[4] Ibid.

[5] Bruce Hoffman, *Inside Terrorism,* New York: Columbia University Press, 1998, p. 174.

Since 1980s, internet has become one of the most popular and effective means of communications, reaching a larger group of audience worldwide. Internet made it possible for an individual to transfer his or her messages with anonymity, effectively and quickly to an almost huge and limitless audience. Nowadays, terrorist groups can disseminate their activities bypassing mainstream media outlets by using internet and different social networking websites. This has helped them reach their audiences in a more clandestine, subtle and safer way. Thus, the volume of recruitment of new terrorists as well as terrorist incidents have increased profoundly in recent years. Although the total number of casualties from terrorism has decreased in recent years, the impact of it remains omnipresent. In 2017, 67 countries witnessed at least one death due to terrorism, which is the second highest number of countries experiencing one death in the past twenty years. In the same year, 19 countries experienced hundred deaths from terrorism and five countries recorded more than a thousand.[6] Online radicalization is a big threat for the countries as online platforms amplified radical messages throughout Western Europe and North America containing Islamophobia and xenophobic sentiments by 50 far-right organizations.[7]

Notably, in 2007, the U.S. Congressional Research Service (CRS) published a report titled *Trends in Terrorism: 2006*. In that report it identifies three new trends of global terrorism: a) the advent of micro-actors with capability of becoming terrorist groups, i.e., reducing the operational capability of terrorist groups, but increase their propaganda, ideological and motivational capability; b) promotion of the sophisticated operational capacity of terrorist groups using modern technology and global information flow (many analysts think that terrorism is becoming a web-directed phenomenon); and c) the increasing nature of overlapping terrorist activities with transnational crime, using same supply, transport and money-transferring networks.[8]

The existing literature on global terrorism suggests that the goals and motivations of terrorist groups vary widely from the particular aim of re-establishing or reuniting a national homeland to the unification of a separated nation. The rapid pace of globalization, the expansion of internet and other communication technologies have helped overcome the time-space constraints for terrorists and brought their war to the 'virtual' level. The current generation is massively influenced by telecommunication technologies, such as internet, mobile phone, and computer. Nowadays, internet and various social networking sites such as Facebook, Twitter and YouTube have become the main sources of communication for terrorist groups.

[6] Institute for Economics and Peace, *Global Terrorism Index 2018: Measuring the Impact of Terrorism*, Sydney, November 2018, available at http://visionofhumanity.org/app/uploads/2018/12/Global-Terrorism-Index-2018-1.pdf, accessed on 09 January 2019, p. 2.
[7] Ibid, p. 47.
[8] Raphael Perl, "Trends in Terrorism: 2006", *CRS Report for Congress,* 12 March 2007, available at https://fas.org/sgp/crs/terror/RL33555.pdf, accessed on 01 November 2018.

Terrorists and insurgents can use such sites to reach their audience bypassing mainstream media. Arguably, a website used by any terrorist group is organized quite similar to any other organization's virtual presence. For instance, website *Al Hesba Discussion Forum* (www.alhesbah.org) or *Syrian Islamic Forum* works as platforms from where viewers from around the world can receive breaking news from Iraq, get links to videos of active extremist campaigns, watch motivational imagery of martyr operatives in heaven, and also download subject-based discussions and speeches.[9] Weimann identifies that today, almost all terrorist groups (more than 40) have their own website and even many terrorist groups maintain more than one website and use different languages.[10] Moreover, terrorist groups nowadays find it difficult to convey their messages through mainstream media channels because of governments' constant vigilance. For example, in 2016, the Government of Singapore banned a newspaper published by a media agency affiliated with the Islamic State (IS).[11] This type of incident may also work as a catalyst for terrorists' resorting to the internet-based alternative media.

On the contrary, the internet-based media also has the potential to work in the global counterterrorism endeavour. For example, in May 2012, the Center for Strategic Counterterrorism Communications of the United States (US) responded within a very short time (48 hours) to counter advertisements promoting extremist violence posted on various internet sites by Al-Qaeda in the Arabian Peninsula (AQAP). The center came with counter-advertisements on the same websites featuring an opposite version of that same message. It also uses various websites, such as Facebook and YouTube, for disseminating counter-narrative messages.[12]

Given this context, the objective of this paper is to examine the role of internet-based alternative media in global terrorism and counterterrorism. The key research questions the paper addresses include: How terrorist groups use internet as an alternative media to reach their audiences? Why terrorist groups resort to the internet-based alternative media? Can internet also be used in countering terrorism? To answer these questions, the paper is divided into five sections. After the introduction, the second section discusses how terrorist groups use internet to reach their audiences. The third section elaborates the causes behind terrorist groups using internet-based alternative media. Section four focuses on the use of alternative media in countering terrorism. The fifth and final section concludes the paper with

[9] Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology", *The Fletcher Forum of World Affairs,* Vol. 30, No. 2, Summer 2006, p. 151.
[10] Gabriel Weimann, "Virtual Disputes: The Use of the Internet for Terrorist Debates", *Studies in Conflict & Terrorism,* Vol. 29, No. 7, 2006, p. 624.
[11] Lim Yan Liang, "Government bans newspaper published by ISIS", *The Straits Times,* 22 July 2016, available at https://www.straitstimes.com/singapore/government-bans-newspaper-published-by-isis, accessed on 08 January 2019.
[12] United Nations Office on Drugs and Crime (UNODC), *The Use of the Internet for Terrorist Purposes*, New York: United Nations, 2012, p.13.

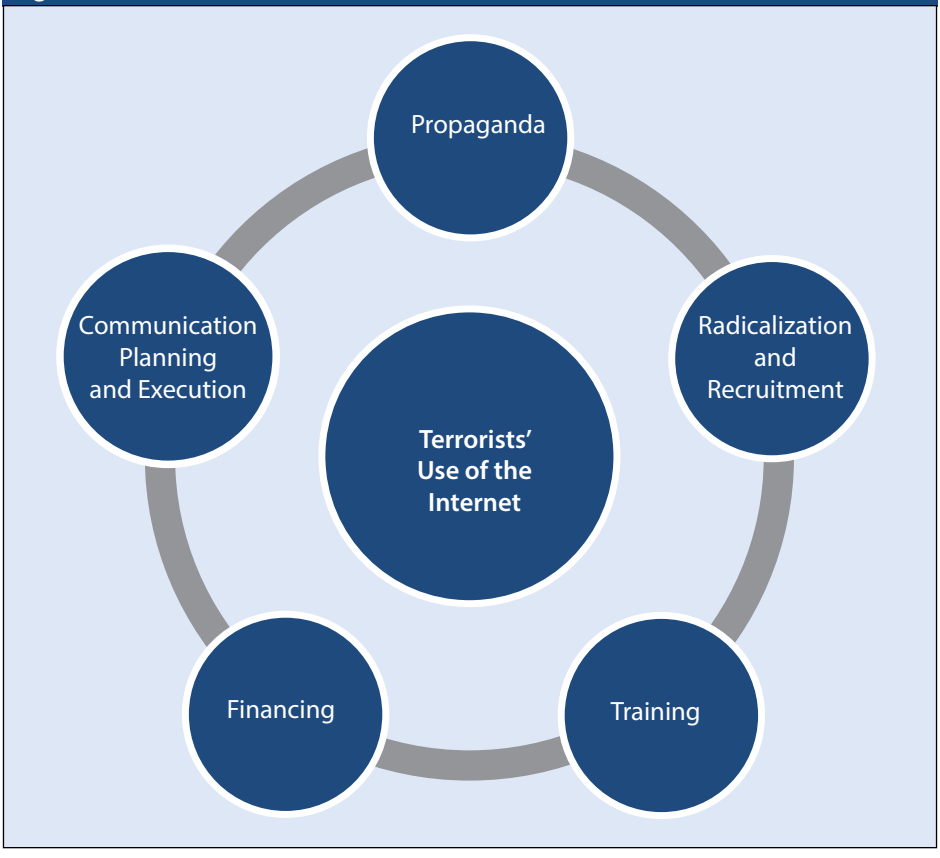
concluding remarks. The paper is primarily a qualitative research based on various secondary sources, including books, journal articles, newspapers and online resources.

2. How Terrorist Groups Use Alternative Media to Reach Their Audiences?

The first terrorist group to exploit the benefits of internet was the Zapatista National Liberation Army (EZLN) which is popularly known as the Zapatistas. Notably, the group is an insurgent movement. It first started using internet to convey its messages in 1990s, and later other insurgent movements and terrorist groups emulated the group's tactics. Nowadays, almost without exception, all major terrorist and insurgent groups have their own websites. A researcher of the US government's Foreign Broadcast and Information Service (FBIS), who works in the effectiveness of internet, has observed, "These days, if you are not in the web, you don't exist".[13] Gabriel Weimann mentioned that "the story of the presence of terrorist groups in cyberspace has barely begun to be told".[14] He found that in 1998, less than half of the thirty terrorist groups that the U.S. State Department designates as Foreign Terrorist Organizations (FTO) had their own websites, but by the end of 1999, nearly all of them have.[15] In 1990s, some technological developments offered terrorist groups an ample opportunity to break the monopoly of commercial and state-owned media. These developments include the use of internet, different types of electronic cheap, video production and editing system and private radio and television stations owned by terrorist groups.[16] Among these developments, the internet undoubtedly brought a phenomenal change for the terrorist groups. The figure below illustrates various usages of internet by terrorists and terrorist groups.

[13] Bruce Hoffman, op. cit., p. 206.
[14] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges,* Washington, D.C.: United States Institute of Peace, 2006, p. 16.
[15] Ibid.
[16] Bruce Hoffman, op. cit., pp. 200-201.

Figure 1: Terrorists' Use of Internet



As can be seen in Figure 1, terrorists mainly use internet for five purposes. These include spreading propaganda through different websites, radicalize potential individuals and recruit them to the respective group, provide training to group members, financing or fundraising and last but not the least communication, planning and executing a particular attack.

Terrorists and insurgent groups utilize internet and use their own media in a subtle way to fulfill their objectives. They use internet for different purposes ranging from disseminating of propaganda to the recruitment, training, financing, planning and execution. In today's world, terrorists can easily broadcast their messages in a simple way. For example, using simple video cameras, terrorists can easily articulate their own messages and then can publish them on their own websites or social media. Moreover, they have ample opportunities to publish whatever they want on their internet sites. There are three major tasks terrorists are doing using the internet: a) adoption of a violent extremist ideology or online radicalization, b) recruitment in

terrorist groups or movements and c) planning and preparation of an attack.[17] Jarret M. Brachman identifies four different ways of using internet by different terrorist groups which include: planning and coordinating movement actions, events and activities, disseminate propaganda and training materials to educate sympathizers, raise and discuss particular topics of interests and news with followers, recruit new members and socialize them, and finally, collect and exploit information about their opponents.[18]

Despite the fact of diversity and multiplicity of terrorist websites, there are a number of common characteristics among them. Usually, these websites have well-designed, colourful, and visually attractive graphics content. These websites chart a particular group's name and its brief history as well as its aims and objectives. In many cases, these sites also contain short biographies of its founders, leaders and key personnel. Terrorist websites usually target three types of audiences: potential and current supporters, global public opinion and enemies.[19] Interestingly, despite comprehensive counterterrorism campaign and the war on terror, the number of extremist websites has grown significantly. Next few paragraphs will shed light on how terrorist groups use internet as an alternative medium to convey messages to their audiences bypassing mainstream media outlets.

2.1 *Spreading Propaganda and Messages to Wider Audience*

Terrorism is a violent action which is conceived primarily to attract public attention and then through the publicity to communicate a specific message. This particular message is called propaganda which is a crucial component of any terrorist group. Indicating the importance of propaganda for a terrorist group, Bruce Hoffman noted, "The terrorist must parlay this illumination (e.g., publicity) into a more effective vehicle of elucidation (propaganda). The centrality of propaganda to this communication process and its importance to the terrorist are self-evident".[20]

In fact, one of the most important and primary purposes of using internet by terrorist groups is to disseminate their propaganda. Terrorist groups usually transform different types of propaganda by providing justifications or promotion of terrorist activities, disseminating ideological or practical instructions and explanations.[21] Their propaganda includes presentations, virtual messages, magazines, audio and video files, treatises and video games prepared by terrorist organizations or their sympathizers. It

[17] Maura Conway, Moign Khawaja, Suraj Lakhani,Jeremy Reffin, Andrew Robertson and David Weir, "Disrupting Daesh: Measuring Takedown Of Online Terrorist Material And Its Impacts", 2017, p. 8, available at http://www.voxpol.eu/download/vox-pol_publication/DCUJ5528-Disrupting-DAESH-1706-WEB-v2.pdf, accessed on 20 September 2018.
[18] Jarret M. Brachman, op. cit.
[19] Gabriel Weimann, "How Modern Terrorism Uses the Internet", *United States Institute of Peace,* Special Report 116, March 2004, p. 1.
[20] Bruce Hoffman, op. cit., p. 198.
[21] UNODC, op. cit., p. 3.

is crucial for any terrorist group to communicate its ultimate intentions behind terrorist activities. In many cases, the mere threat of terrorist acts can serve the same purpose of an actual incident if it can generate the similar fear in the psyche of a target audience. In fact, without properly disseminating the terrorists' causes, the corresponding impact would be substantially reduced.[22]

A common feature of terrorism-related propaganda is the promotion of violence. Internet provides terrorist groups with multiple opportunities to convey their messages, which reduce their reliance on traditional media channels and news services. Internet-based propaganda is handy for terrorist groups and it may include various contents, such as video footages of terrorist acts or video games developed by terrorists, it may encourage their audiences to engage in a role-play experience by acting the same role as a virtual terrorist. Another aspect of their propaganda is the promotion of extremist rhetoric, which is another common trend of ever-growing internet-based platforms. The use of propaganda by terrorists is mainly aimed at their actual supporters or followers who may focus on incitement or radicalization to terrorism, recruit new personnel to their network, convey their messages to others and accomplishment in extremist goal. Moreover, their propaganda is also crucial to demonstrate the effective execution of terrorist activities to their financial supporters. For instance, the Liberation Tigers of Tamil Eelam (LTTE) was one of the first groups to spread the group's propaganda.[23] When the civil war broke out between the LTTE and Sri Lankan government, it led to a large number of Tamil diaspora around the world, particularly in countries like the US, the United Kingdom (UK), Australia, France and Canada. In this regard, the internet played a vital role for the LTTE to inform the situation to the diaspora and simultaneously spread the group's propaganda. The Tamil diaspora also spreads the group's propaganda to the world.[24]

2.2 *Radicalization and Recruitment of Manpower*

Different terrorist groups use internet not only as a means of passing their extremist rhetoric, ideologies and videos but also to develop a relationship with the solicit support base for their targeted group. Usually, terrorists use platforms, such as password-protected websites and restricted chat groups as a clandestine means of personnel recruitment. Access to internet has helped the extremist and terrorist groups recruit a new workforce from a global scope of potential recruits. Prior to the recruitment, terrorist groups primarily target marginalized segment of a society and the process of radicalization and recruitment generally capitalizes on individual sentiments of exclusion, injustice or humiliation.

[22] Bruce Klopfenstein, op. cit., p. 107.
[23] Jasmine Jawhar, *Terrorists Use of the Internet: The Case of Daesh*, Ministry of Foreign Affairs: Malaysia, 2016, p. 33.
[24] Peter Chalk, "The Tigers Abroad: How the LTTE Diaspora Supports the Conflict in Sri Lanka", *Georgetown Journal of International Affairs,* Vol. 9, No. 2 (Summer/Fall), 2008, pp. 97-104.

Notably, terrorist groups spread propaganda to the targeted segment of a society through various innovative ways. Popular music videos, cartoons and computer games are considered to be the most popular means used by terrorist groups to recruit new personnel to their gang. They make cartoons and stories with messages that glorify the act of terrorism, which inspire newcomers to perpetrate terrorist and suicide attacks. Some terrorism experts opine that online forums help novices to virtually interact with 'trainers' which help them successfully separate the wheat from the chaff and help them to gather experience on bomb-making and to some extent weapon handling.[25] Since the 9/11 incident, a new trend is evolving as terrorist groups inspire their potential recruits through different types of online communications and motivate them to execute terrorist activities. Moreover, along with aiding in planning and executing terrorist attacks, today's terrorist groups provide a database of information to internet to know more about terrorist organizations and their aims and objectives.[26]

It is also evident that online recruitment materials are often translated into different languages including English and French. Terrorist groups usually do it to attract supporters in western countries. This method used by Al Qaeda and other terrorist groups has been proven much effective and terrorist groups have become successful in transforming many ordinary people into obedient actors who carry out terrorist acts on command.[27]

2.3 *Financing for Terrorist Activities*

Nowadays, terrorist groups use internet as a fundraising platform for acts of terrorism. Sympathizers of terrorist groups usually undertake the fundraising activity in four different ways: e-commerce, direct solicitation, through charitable organizations and through hacking or exploiting of various online payment tools. Hence, e-commerce refers to the online-based businesses run by terrorist groups, stores offering audio and video recording, books and other items for their supporters. Direct solicitation refers using the websites, mass mailings, chat groups and selected communications to request donations from sympathizers and supporters of terrorist groups. Fund transfer to certain terrorist groups is usually done electronically between different groups in various ways, including electronic wire transfer, credit card or alternative payment facilities available via services like Skype or PayPal. Terrorist groups sometimes exploit payment methods through

[25] Michael Kenny, op. cit.

[26] Dana Janbek and Valerie Williams, "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism", *The Brown Journal of World Affairs,* Vol. XX, Issue 11, Spring/Summer 2014, p. 298.

[27] Rosanna E. Guadagno, Adam Lankford, Nicole L. Muscanell, Bradley M. Okdie and Debra M. McCallum, "Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research", *Revue internationale de psychologie sociale,* Vol. 23, No. 1, 2010, pp. 25-56, available at https://www.cairn.info/revue-internationale-de-psychologie-sociale-2010-1-page-25.htm, accessed on 07 October 2018.

identity theft, credit card theft, stock fraud, wire fraud, auction fraud or intellectual property crimes.[28]

To find out a potential donor, terrorists or terrorist groups take the assistance of internet user demographics which allow them to identify users having sympathy to a particular issue or cause. Then these people are asked to make donations, usually through emails sent by a front group (an organization which supports the terrorists' aims, but operates legally and publicly having no direct link with the terrorist organization).[29] Mentionably, financial support to some charity organizations are also used for illicit purposes. Terrorist groups claim humanitarian support hiding their identity while they use the fund for terrorist purposes. Some groups who use their charitable organizations for terrorist funding include the Global Relief Foundation, Benevolence International Foundation and the Holy Land Foundation for Relief and Development. All of these groups use fraud method to finance terrorist groups in the Middle East.[30] Even for Irish Republican Army (IRA), visitors can make credit card donations in the group's own website.[31] In a nutshell, internet offers a global reach and a certain degree of security and anonymity for both donors and recipients.[32]

2.4 *Providing Training*

Terrorist groups often resort to internet for providing training to terrorists. Brynjar Lia considers that training is very important for terrorist groups and she labels it as the primary vehicle using which different terrorist groups become able to transform their radical ideologies to violent attack.[33] The most organized terrorist group in producing training material for the new recruits in the online is AQAP. It has been publishing its own magazine named *Al-Battar Camp (mu'askar al-battar)* on the bi-weekly basis since 2004. The magazine usually provides both ideological articles and articles on the first-hand military skills.[34] AQAP also published an online newspaper named *Inspire* with the objective of inspiring young people to train terrorist tactics from their home. The newspaper contains a good amount of ideological material and incorporated inspirational messages of the top Al Qaeda leadership, Osama Bin Laden, Ayman al-Zawahiri and other key figures. The newspaper is an inspirational platform for terrorists, which, for example, motivates an individual to launch an indiscriminate attack from a tower or kill a government official to draw more attention.[35]

[28] UNODC, op. cit., p. 7.
[29] Gabriel Weimann, "How Modern Terrorism Uses the Internet", op. cit., pp. 7-8.
[30] UNODC, op. cit., p. 7.
[31] Gabriel Weimann, "How Modern Terrorism Uses the Internet", op. cit., p. 7.
[32] Michael Jacobson, "Terrorist Financing on the Internet", *CTC Sentinel,* Vol. 2, Issue 6, June 2009, p. 17.
[33] Brynjar Lia, "Doctrines for Jihadi Terrorist Training", *Terrorism and Political Violence,* Vol. 20, Issue 4, pp. 518-542.
[34] Thomas Hegghammer, "Terrorist Recruitment and Radicalization in Saudi Arabia", *Middle East Policy,* Vol. XIII, No. 4, Winter 2006, pp. 39-60.
[35] UNODC, op. cit., p.8.

Although terrorist groups like Al Qaeda and IS have no virtual training camps, online training courses organized by the *Jihobbyists* provide an opportunity for newcomers to learn more about the operational activities of global jihad. In these days, the e-learning courses of Al Qaeda are more organized than the past, which contain more audio-visual materials, as well as written learning materials. Previously, Al Qaeda transmitted its ideology and training through direct contact but from the 1990s, the terrorist group started documenting its training materials. The most notable work is the *Encyclopaedia of Jihad,* which is the first collection of that type. This one is primarily a collection of all written experience of the veterans of the Afghan-Soviet jihad to make sure that their knowledge is not lost for the future jihadists.[36] *The Encyclopaedia of Preparation* probably is a comprehensive collection of internet-based training manual. The editor of this encyclopedia is a person whose nickname is Ibn Turab, who was previously an active member of Al Qaeda's radical forum *al-Ma'sada al-Jihadiyya*.[37] The editor of the encyclopedia mentioned that the purpose of writing the encyclopedia is to improve the military knowledge for mujahedeen to enable them to re-establish the Caliphate (Encyclopedia of Preparation). The online training material provided in this encyclopedia was not prepared for a specific region or group. The origin of the documents used in the encyclopedia comes from diversified sources: manuals written mainly by the Afghan war veterans and some other written by the Palestinian veterans and a couple of internet activists with the least battle experience. However, there are many instructional videos available online are mainly produced by another group, Hezbollah.[38]

The Islamic Media Centre (IMC) is another well-known media outlet to issue training materials for terrorists. It has been working since the 1990s and broadcasting training materials on CDs and later through internet. Oussama Kassir, one of the key figures of the IMC has an allegation of taking training from Lebanon, Afghanistan and Kashmir and fighting in Afghanistan against the Union of Soviet Socialist Republics (USSR). He visited the US in 1999 with a view to setting up a training camp in the US, along with some other key figures like Abu Hamza and others. Moreover, since 2002 he has been operating various websites linked with the IMC.[39] The IMC had wide network and access to numerous materials written by experienced commanders. Moreover, for their sympathizers, they translated a large number of US Army Field Manuals into the Arabic language.

Online instruction materials also include various tools to facilitate counterintelligence and hacking tactics to ensure the safety and security of illegal communications and online activity with available encryption materials and anonymizing

[36] Ali H. Soufan, *The Black Banners: The Inside Story of 9/11 and the War Against Al-Qaeda,* New York: Norton, 2011.
[37] Anne Stenersen, "The Internet: A Virtual Training Camp?", *Journal of Terrorism Research*, Vol. 3, No. 2, p. 218.
[38] Ibid.
[39] Thomas Hegghammer, op. cit., p. 41.

tactics. Internet network helps terrorist groups build a sense of virtual community among individuals from all over the world, encouraging the creation of new networks for the distribution of instructional and inspirational materials.

2.5 *Communication, Planning and Execution*

The history of criminology suggests that nowadays almost every terrorist incident involves the use of internet technology. Use of internet becomes crucial for terrorist groups when planning of a terrorist incident involves remote communication among multiple actors. In some cases, terrorist groups use internet to successfully identify a potential target for a terrorist attack. The planning and execution process includes obtaining instructions of attack to collect available information from different sources about the possible target. Multiple uses of internet to bridge distances and scattered geographical areas and a vast amount of public information on internet made it a key tool in planning and executing terrorist activities.

Use of internet has also facilitated terrorist groups to execute different terrorist activities with more accuracy. For instance, explicit threats of violence, including the threat of using weapons may be transmitted through internet to generate fear or panic among mass people. Internet technology also has facilitated the acquisition of weapons, explosives or other materials necessary for the execution of an attack. Sometimes terrorists use e-commerce service to purchase required materials. In some cases, terrorist organizations undertake cyber attacks by deliberate exploitation of the computer networks.

Terrorists also use internet while communicating during the process of planning a particular attack. An example can be provided in this regard. Najibullah Zazi, responsible person for planning an attack on the New York subway system in 2009, communicated with his contact in Pakistan using email to outline the attack. In addition to that, another person involved in the incident from the UK exchanged messages regarding the making of bombs and the progress of the plot using coded language. This example illustrates that internet was used by terrorists to communicate details of planning and executing the attack.[40]

3. Why Terrorist Groups Use Alternative Method to Promote Their Causes?

Although in recent years, terrorist groups get most of the instructions and training materials from online sources, till date there has been few numbers of empirical criminology researches have been done on the topic. However, one key aspect is clear that both terrorism and internet impact profoundly in contemporary terrorism studies and they often shake our everyday life and the functioning of the micro and macro level

[40] Dana Janbek and Valerie Williams, op. cit., p. 301.

economic, social and political systems.[41] Previously, terrorist groups used three main ways to conduct their communication process: a) clandestine or rebel radio stations b) underground posters, newspapers, flyers and other publications, and c) commercial, conventional or state-owned media (e.g., radio, television and newspaper).[42] Gabriel Weimann identifies some reasons which work as catalysts for terrorist groups in using internet. These are:

- Anonymity while communication;
- Easy access;
- Devoid of regulation, censorship or any sort of government control;
- Easy to reach huge audiences throughout the world;
- Fast and free flow of information;
- Inexpensive development and maintenance of a web presence;
- Interactive medium;
- A multimedia environment; and
- The ability to shape coverage in the traditional mass media, which increasingly uses internet as a source for stories.[43]

In the post 9/11 era, numerous counterterrorism campaigns have forced terrorists to rely more on online methods rather than practical training courses. In recent years, terrorist groups in the West and elsewhere are using internet to collect information and communicate among themselves. Previously, different terrorist groups transferred their knowledge and training through direct contact in a training camp or similar settings. However, nowadays, terrorist organizations are trying to do that in an alternative way. There is a good number of websites which provide terrorist groups' a platform for disseminating various online resources: audio and video clips, online manuals, advice and information, etc. To some extent, internet-based platforms provide instructional materials in an easily accessible multiple language and multiple formats; topics such as the way to join terrorist groups; instructions for preparing home-made explosives, weapons, firearms or other hazardous materials; and ways to successfully plan and execute a terrorist incident.[44] In the next few paragraphs, some background causes of using internet by terrorists and terrorist groups are discussed briefly.

[41] Gary LaFree, "Terrorism and the Internet", *Criminology & Public Policy*, Vol. 16, Issue 1, 2017, pp. 1-6.
[42] Bruce Hoffman, op. cit., p. 199.
[43] Gabriel Weimann, "Virtual Disputes: The Use of the Internet for Terrorist Debates", op. cit., p. 624.
[44] UNODC, op. cit., p. 8.

3.1 *Maximizing Safety and Avoiding Counterterrorism Campaign*

Maximizing safety and security of terrorists and avoiding the pressure of counterterrorism campaigns are perhaps the main reasons for adopting more online-based training exercises. Terrorist groups, nowadays, can use many sophisticated methods which make it difficult to identify a perpetrator, content or recipients of a particular internet-based communication. Identity hiding options like encryption tools and some anonymizing downloadable software can be found on internet. These types of modes usually hide the unique Internet Protocol (IP) address and help to conceal a user's identity, location, a route to access the internet and other important information. These types of activities make it difficult for organizations and people engaged in counterinsurgency activities to find out the perpetrators of terrorist incidents. In some instances, terrorists use steganography, which helps them transfer messages hiding in images.

In these days, numerous counterterrorism campaigns have forced terrorists to rely more on online methods rather than practical training courses. In recent years, terrorist groups in the west and elsewhere are using internet to collect information and communicate among themselves. Previously, different terrorist groups were used to transfer their knowledge and training through direct contact in a training camp or similar settings. However, nowadays, terrorist organizations are trying to do that from an alternative way. There are good number of websites, which provide terrorist groups a platform for disseminating various online resources: audio and video clips, online manuals, advice and information, etc.

Even before the 9/11 incident, Al Qaeda and other terrorist groups had a tendency of exploiting the advantages of modern technologies. Al Qaeda leaders Osama Bin Laden and Ayman al-Zawahiri recognized the importance of these developments. Especially, Osama Bin Laden noted the satellite-based propaganda and rhetoric, both are equally important as cruise missiles and unmanned bombers.[45] Al Qaeda's virtual dependency even became more central to its strategy after losing its Afghan base. Peter Bergen, therefore, labelled this strategy of Al Qaeda as "Al Qaeda 2.0." [46]

3.2 *Easy Mode to Transfer Terrorist Ideology*

Internet has become one of the easiest and safest modes to spread terrorist ideology. Nowadays, the battlefield is no longer the primary place for war. Rather the net-based warfare is now the eminent battleground. Anyone using internet can connect YouTube and other social networking websites from anywhere around the world to upload as well as download videos to share an ideology with local communities, diaspora and to the rest of the world. The online-based media provides a comparatively safe mode

[45] Marc Lynch, "Al Qaeda's Media Strategies", *The National Interest,* No. 83, Spring 2006, pp. 50-56.
[46] Ibid.

for the dissemination of radical ideas unlike conventional communication tools, such as books, newspapers, leaflets or VCDs as it does not leave any kind of physical evidence and is a more reliable mode to reach a much wider range of audience.[47] Nowadays, internet is flooded with contents pertinent to extremism and terrorism. Table 1 provides an idea about the quantities of radical materials available online:

Table 1: Google Search Results of Critical Keywords Related to Extremism

Search Term	Number of Results
"how to make a bomb"	1,830,000
"beheading video"	257,000
'Salafi publications"	46,200

Source: Ines von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon, Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism, 2013, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf, accessed on 14 November 2018, p. 3.

The table indicates that these days internet is flooded with terrorist contents easily accessible to all. If terrorists have access to internet, they tend to get the advantage of technology. By using online method they can reach a wide range of their audience, which is quite impossible through the oral tradition developed over the years. For example, terrorist groups in Iraq pass their messages through online that constantly goes up and down. They try to convince the Iraqi population that their insurgency method is doing better. This is how terrorist groups manipulate the advantages of internet.

Similar to Al Qaeda, terrorist group IS is also harnessing the advantages of internet technology. The group controls a small territory in Syria and Iraq. However, social media connects it with the whole world within the reach of every cell phone, desktop and laptop computer.[48] In fact, IS also extracts the benefits of advanced technologies to reach its audiences in a more effective way. The group has several thousand online activists to support their causes who work in a more disciplined way. For example, if any one of the group posts a particular content to internet–say an authentic video of the beheading, then the second tier of online activists take it to Twitter to retweet the content with a hashtag and also retweet each-other's tweet and this type of online hashtag campaign ultimately creates a "Twitter storm". In addition to that, other members of the group upload the content to other online platforms that it remains available on internet. This online campaign has favoured them a lot and attracted supporters from all over the world.[49]

[47] Virginie Andre, "Neojihadism' and YouTube: Patani Militant Propaganda Dissemination and Radicalization", *Asian Security*, Vol. 8, No. 1, 2012, pp. 27-53.
[48] Christopher S. Stewart and Mark Maremont, "Twitter and Islamic State Deadlock on Social Media Battlefield", *The Wall Street Journal,* 13 April 2016, available at https://www.wsj.com/articles/twitter-and-islamic-state-deadlock-on-social-media-battlefield-1460557045, accessed on 08 January 2019.
[49] Hisham Melhem, "Keeping Up with the Caliphate: An Islamic State for the Internet Age", *Foreign Affairs,* November-December 2015.

In recent years, along with various terrorist groups, lone wolf terrorists[50] are also using internet to spread terrorism. Notably, lone-wolf terrorism has become one of the fastest growing terrorist categories in recent years. Europol published a terrorism situation and trend report in April 2012, which highlighted the propensity of using internet by terrorists. The report narrated that for extremist groups, internet has become the 'principal means of communication', therefore, their 'substantial online presence' is viewed. Besides the use of propaganda, fundraising, planning and recruitment, terrorist groups use internet for 'cyber attacks' on the operating systems of the European Union (EU) member states.[51]

Terrorists and terrorist groups tend to harness the opportunities of the interactive capabilities of internet, including instant messenger, blogs, chat rooms, video sharing websites and other social networks. A statistic suggests that in these days about 90 per cent of the terrorist incidents occur using the social networking websites whether it is Paltalk, independent bulletin boards or Yahoo.[52] These social networking sites help terrorists to hide their identities and create direct contact with perpetrators or mastermind of a terrorist attack. The massive expansion of the lone-wolf terrorists in these days poses a major challenge to the issue of counterterrorism steps. In fact, the lone-wolf terrorists offer a nightmare for organizations who work for counterterrorism. According to Global Terrorism Index 2017, terrorist groups exploit internet and social media, mainly to influence public opinions, instigate communal tensions, radicalize young people and recruit cadres and cyber warriors to carry out cyber espionage, cyber-attacks and hacking.[53] A RAND corporation research outcome suggests that internet enhances opportunities to make people radicalized as it is easily accessible to many people. The second aspect it found that internet acts as an 'echo chamber' for extremist beliefs.[54]

There are some other reasons for using internet by terrorist groups. Bilveer Singh states that internet helps terrorists bypass national laws. Terrorists tend to take advantage of the weak legal system to spread terrorism where internet works as a unique platform for them.[55] He gave an example of Indonesia and noted that

[50] This type of terrorists are individuals or a small group of individuals who are radicalized through the internet and are ready to plot the preparation for attacking in the dark. In recent years, the lone-wolf terrorists are flourishing in many countries, including the US, France, Germany, Canada, Italy, Spain, Denmark, Portugal, Great Britain, Sweden, Norway and Poland.

[51] Gabriel Weimann, "Lone Wolves in Cyberspace", *Journal of Terrorism Research,* Vol. 3, Issue 2, Autumn 2012, p. 80.

[52] Ibid., p. 84.

[53] Institute for Economics and Peace, *Global Terrorism Index 2017: Measuring and Understanding the Impact of Terrorism*, p. 100, available at https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf, accessed on 01 November 2018.

[54] Ines von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism, 2013,* available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf, accessed on 14 November 2018.

[55] Bilveer Singh, "Countering Online Extremism – A Perspective on the Indonesian Case", Lecture given at the Workshop on Extremism and Terrorism Online: A Multidisciplinary Examination

the country's legal system is relatively weak to deal online radicalization which led to terrorists taking advantage of the situation.[56] According to Jasmine Jawhar, many reasons why terrorist groups use internet including: easy access to internet with little technical knowledge of making a website, anonymity of communication, communicating with like-minded people, an easy source of revenue where donations can be obtained bypassing national law, etc.[57]

4. Use of Alternative Media in Counterterrorism

Despite the fact that terrorist groups have developed many routes to use internet as an alternative media, it also provides an ample opportunity for gathering intelligence and other activities to prevent and counter the threats of terrorism. Internet helps gather evidence for bringing terrorists under jurisdiction. Moreover, frequent use of internet by potential terrorists unintentionally makes themselves visible in front of the national and international counterterrorism community.[58]

The EU model can be a good example for countries using internet as a tool in combating terrorism. The EU Internet Forum was launched in 2015 with a view to stopping the use of internet by terrorists. Notably, the EU Internet Forum was comprised of EU Home Affairs Ministries, the internet industry and all other related stakeholders with a view to working in a partnership to address the complex problem and protect the citizens of the EU. The forum started its journey with two main objectives: to restrain accessibility to terrorist content online and to enable the civil society that it can help increase the volume of effective counter-narratives online. On December 2016, at the EU Internet Forum, internet companies announced the creation of a shared 'Database of Hashes' to detect more proficiently terrorist elements on social media. On the same occasion, the EU Civil Society Empowerment Programme was initiated to develop effective counter-narrative campaigns. To that end, the EU allocated €6 million in support of those campaigns.[59]

The US also deployed its law enforcement, intelligence and different security agencies in countering terrorism by increasing surveillance on communications and online activity. Particularly the Joint Terrorism Task Force (JTTF) has increased partnerships from 35 to over 100. According to the Federal Bureau of Investigation (FBI), "JTTFs have been instrumental in breaking up cells…[and] they've foiled attacks on the Fort Dix Army base of New Jersey, on the JFK International Airport in New

of Current Trends and Challenges, 14 October 2014, Singapore, cited in Jasmine Jawhar, op. cit, p. 19.
[56] Ibid.
[57] Jasmine Jawhar, op. cit.
[58] Dana Janbek and Valerie Williams, op. cit.
[59] European Commission, "Fighting Terrorism Online: Internet Forum Pushes for Automatic Detection of Terrorist Propaganda", 06 December 2017, available at http://europa.eu/rapid/press-release_IP-17-5105_en.htm, accessed on 01 October 2018.

York, and on various military and civilian targets in Los Angeles."[60] Moreover, the FBI has taken its investigative approach to more intelligence-led strategies and proactive nature to combat terrorist attack prior to the real incident. It implements a number of undercover tactics on internet. For example, it creates parallel terrorist recruiting websites which are convincing enough to attract potential terrorists. A testimony of the US' proactive role can be found from Abdella Ahmad Tounisi's case. When the 18-year old young man was searching internet for terrorist group Jabhat al-Nusra, an Al Qaeda branch in Syria, he found a site which was created and maintained by the FBI. When Tounisi communicated the website's recruiter, who was originally an FBI agent, both of them exchanged email messages and the teen revealed his plan to engage in jihad in Syria. In the end, the FBI became able to arrest Tounisi in 2013 at Chicago O'Hare International Airport just before his departure to Syria.[61] However, online surveillance has become a concern for citizens and civil society organizations in the US. The National Security Agency (NSA) of the country was accused of engaging in online surveillance without any specific allegation or merely based on individual suspicion and spying on the country's citizens despite its commitment to monitoring only specific foreign citizens.[62]

Sometimes, terrorists are well-prepared and have better technological know-how than law enforcement agencies. Even the bureaucracy of the US government could not protect the country's cyberspace from the terrorists' hand. Notably, the current US government strategy to combat terrorist use of internet started in 2007 when Twitter was in its initial age and earlier than Snapchat, WhatsApp, Telegram and many other popular social networking sites were created. According to the FBI website, the bureau could not get access to the contents of about 7,800 devices in 2017 due to encryption blockage, it was more than half of the device it attempted to access during that time frame.[63] Therefore, a new form of counterterrorism cyber strategy is needed to combat this new challenge. In this regard, governments can form special intelligence units where researchers and experts need to be included along with anti-terrorism agencies which may prove effective in preventing and controlling the online-based terrorism. For example, the Government of Bangladesh has introduced 'Digital Security Act 2016' to prevent internet-based crimes committed using a computer, computer system or network, mobile phone or any kind of digital communication media whether voice or data. This Act also enables the government to establish a Digital Forensic Lab for properly investigating internet-based crimes.[64]

[60] Federal Bureau of Investigation (FBI), "Joint Terrorism Task Forces", available at https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces, accessed on 02 October 2018.

[61] Dana Janbek and Valerie Williams, op. cit., pp. 302-303.

[62] Alex Adbo and Jameel Jaffer, "How the NSA's Surveillance Procedures Threaten Americans' Privacy," Free Future, 21 June 2013, available at https://www.aclu.org/blog/national-security/secrecy/how-nsas-surveillance-procedures-threaten-americans-privacy, accessed on 05 February 2019.

[63] Federal Bureau of Investigation (FBI), "Director Addresses 'Going Dark' Problem at Cyber Conference," available at https://www.fbi.gov/audio-repository/ftw-podcast-wray-going-dark-iccs-011118.mp3/view, accessed on 18 November 2018.

[64] Md Sazzad Hossain, "Social Media and Terrorism: Threats and Challenges to the Modern Era", *South Asian*

Arguably, tackling the terrorists' use of cyberspace requires a multi-faceted approach involving governments, civil society, international organizations and the private sector. Realizing the importance of the fact, on 20 September 2017, Italy, France and the UK co-hosted a United Nations High-level Meeting on *Preventing Terrorist Use of the Internet*. And the participants were French President Emmanuel Macron, Prime Minister of Italy Paolo Gentiloni, British Prime Minister Theresa May and Senior Vice President and General Counsel of Google Kent Walker. Mentionably, the meeting was held on the sideline of the 72nd UN General Assembly. The effort was initiated by the Counter-Terrorism Committee Executive Directorate (CTED) of UN Security Council, and for the first time, the global community witnessed an initiative where the global leaders and technology executives addressed at the United Nations on a very important issue.[65] The high-level meeting encouraged governments and civil society to engage with the Global Internet Forum for Counter Terrorism (GIFCT) which was launched by Microsoft, Facebook, Twitter and YouTube on 26 June 2017. Since its inception, GIFCT has been playing the role of a global focal point in combating terrorism in the digital battlespace. This type of initiative is setting the tone of combating terrorists in the cyberspace. UK Prime Minister Theresa May commented that the initiative works "as evidence of the commitment held by governments, companies, and civil society in collaborating to protect citizens against the use of internet by terrorists to spread their ideology".[66]

The global initiative is also reflected in the activities of the UN Security Council. The Security Council Counter-Terrorism Committee is working to address various problems emanated from the abuse of Information and Communication Technologies (ICT) by terrorists and terrorist groups. To that end, the committee is guided by several Security Council Resolutions. Among the resolutions, probably the most important one is the Security Council Resolution 1373 (2001) which calls on all members of the UN to find ways to enhance and accelerate the exchange of information regarding the use of ICT by terrorist groups and to suppress terrorist recruitment. Microsoft also informed the committee that it had made provisions to prohibit the posting of terrorist contents by organizations included in the Consolidated United Nations Security Council (UNSC) Sanctions List.[67]

Survey, Vol. 22, No. 2, 2015, pp. 148-149.

[65] Security Council Counter-terrorism Committee, "CTED Initiated Process Results in High-level Meeting on Preventing Terrorist Use of the Internet", available at https://www.un.org/sc/ctc/news/2017/09/21/cted-initiated-process-results-high-level-meeting-preventing-terrorist-use-internet/, accessed on 19 November 2018.

[66] Ibid.

[67] Security Council Counter-terrorism Committee, "Information and Communication Technologies (ICT)", available at https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/, accessed on 19 November 2018.

5. Concluding Remarks

Use of internet-based alternative media for terrorist purposes is one of the key features of contemporary terrorism studies. This study reveals that in these days terrorist groups are more dependent on internet for spreading their terrorist ideology than the mass media to disseminate their causes. Especially, the 'lone-wolf' terrorists are motivated and trained by the social media to conduct terrorist incidents on a larger scale. Terrorist organizations use their own media for several purposes, which include spreading terrorist propaganda, radicalization, recruit and train a new workforce, fund mobilization, communication, planning and executing terrorist operations. It is also evident that most of the online materials are produced by sympathizers rather than the key leaders of Al Qaeda, IS or other terrorist groups. Particularly, in recent years, due to extensive counterterrorism initiatives and drone strikes, terrorist groups are using internet to train their sympathizers on bomb-making and other operational activities. To that end, Al Qaeda, IS and other terrorist groups are using their own websites as well as various social networking sites to reach their audiences independently from mainstream media outlets.

Although internet is considered to be a prime platform for training and spreading the terrorism, internet or online mode is yet to completely replace the offline or practical mode for spreading the terrorism and to become a virtual training camp. In reality, internet has more inspirational role than the operational impact to the sympathizers. Till date, terrorist groups rely heavily on offline methods to recruit and train a new workforce because practical technological knowledge is more important than theoretical knowledge, which is available on internet. Further studies in this field can reveal the implications of internet on spreading terrorism.

Terrorism, in every aspect, affects the whole global community. The use of internet by terrorist groups disregards national borders, amplifying the potential impact on the sufferers. However, there is no scope to deny the fact that the terrorist sympathizers are using internet and social networking sites to attract the young generation. Therefore, to prevent the dissemination of terrorist and violent extremist ideology, international actors along with industry and law enforcement agencies need to work together to make the cyberspace a hostile environment for the terrorists. And it is also evident from empirical evidence that internet-based alternative media also can help in counterterrorism endeavours.

BOOK REVIEW

Analysing China's Soft Power Strategy and Comparative Indian Initiatives by Parama Sinha Palit, published by SAGE Publications, India Pvt Ltd, New Delhi, 2017, XXIV+368 pages.

In global discussion on international and strategic relations, soft power has gained considerable currency. A country's soft power is not only dependent upon its global image but also global image of a country is enhanced by it. Currently, great power, rising power as well as small power are exploring their soft power to play a major role in global affairs. As rising powers, China and India are trying to develop their soft power. China uses different soft power tools, such as setting up Confucius Institute across the world, undertaking regional connectivity initiatives, granting more scholarship for foreign students, investing in infrastructure, providing humanitarian assistance, etc. to gain its foreign policy objectives. Likewise, India also uses various soft power tools, e.g., Bollywood movies, diaspora community, cuisines, tourism, secular values, etc. Thus, *Analysing China's Soft Power Strategy and Comparative Indian Initiatives* brings to light China's consummate efforts in correcting adverse global perception produced by its strategic rise through extensive use of soft power. In this book, Parama Sinha Palit inclusively focuses on the vigorous deployment of China's soft power, the distinct nuances and variation visible across countries and regions. Moreover, to provide a comparative understanding of India and China's soft power initiatives, it also reflects on the recent developments of soft power initiatives in Indian foreign policy.

The book spans a total of 368 pages, including a preface followed by eleven chapters divided into three parts. It is the outcome of Parama Sinha Palit's motivation to study modern China's extensive deployment of soft power to gain its core strategic goals during her visit to various parts of China and fascinating interaction with Chinese scholars and experts.

The central theme of the book is evolution and application of China's soft power. Though China is the context, subject and discussion of the book, it also provides a comparative analysis of China and India's soft power initiatives to understand Sino-Indian relations. In the preface, the author gives several important arguments: China's soft power coexists with hard power which reflects a duality inherent in Chinese diplomacy and foreign policy, Chinese soft power is characterized by its pronounced economic content and Chinese soft power has entailed more of cultural diplomacy than public diplomacy, India's soft power will encounter formidable challenges, probably more than what China does, etc. Following the preface, part one 'Soft Power and China' comprehensively discusses the concept of soft power. Part two 'Chinese Soft Power: Regional Studies'

illustrates the regional variations of China's soft power strategies. Part three 'Soft Power, China-India Engagement and Comparative Dimensions' focuses on various India's soft power initiatives and compare them with China's initiatives. It also analyses Sino-Indian relations from the perspective of soft power.

To set the context of the analysis of China's soft power, the author devotes a significant concentration on the concept of soft power. It argues that although the term soft power was first coined by Joseph Nye Jr., it can hardly be described as a product of contemporary western thinking. In this respect, on the one hand, it provides ample evidences of the historical existence of soft power in the foreign policy of China and India. It explains the root of soft power as an idea in China's foreign policy can be traced during spring and autumn era 771-476 BC, a period known as the 'Hundred School of Thoughts'. Thinker of that period like Kong Zi, Confucius and Mencius denounced war and preferred diplomatic maneuvering over military confrontation in achieving state interests. In ancient Chinese literatures, ideas such as 'culture winning over an enemy' and 'winning a battle before it is fought' are rampant. Similar to Chinese literatures, ancient Indian literatures, e.g., *Mahabharata, Manu Smriti* and *Arthashastra* provide a peek into ancient Indian cultural tradition and practice of diplomacy for conducting international relations. Noted scholars of the time like Kautilya and Kamandak have also referred to soft diplomacy for achieving progress. On the other hand, little illustration is provided on the concept of western influential thinkers, such as E.H. Carr, Foucault, Bourdieu, Gramsci, Habermas and particularly Nye who have variously articulated soft power, albeit in implicit and contextual fashions. As the author tries to de-Americanize the concept of soft power, greater exemplification on both western and non-western concept of soft power is crucial. Thus, extensive discussion on western soft power concept by identifying similarities and dissimilarities between the two discourses could enrich the conceptual part of the book further.

The book is mostly dedicated to trace several tools of China's soft power to gain foreign policy objectives. It identifies several tools of China's soft power, e.g., economic engagement (investment, aid, loan and grant); cultural diplomacy; public diplomacy; education and media, etc. It argues culture as the core of soft power finds increasing resonance in China's conduct of external engagement. Culture has been inseparable from politics in China and also considered as third pillar of Chinese diplomacy after economics and politics. Thus, the book highlights the prominent role of culture in China's approach to soft power. Apart from culture, by posing as the locomotive for regional growth and prosperity, China has effectively employed economic tools as one of its major soft power instruments. It further explains the unique approach of China's soft power strategy in combining the 'traditional' and 'modern' tools for connecting to people. China has imparted the typical Chinese flavour to soft power by combining cultural

initiatives and public diplomacy with economic engagement, buoyed by efforts to build people to people contacts through education and an active role of its media agencies. Parama delves into China's pursuit of cultural diplomacy and several other soft power tools in connecting China with rest of the world but additional observation on public diplomacy could be considered given the fact that public diplomacy had a somewhat late start and is progressing recently in China.

A big focus of the book is discussion of the regional variations of China's soft power strategies. Part two of the book goes on to explain that these regional variations have interesting nuances in securing China's fundamental strategic objectives of providing economic progress to a huge populations, accessing to critical natural resources, maintaining a stable external environment particularly in neighbourhood, projecting a 'benign' external images, etc. Part two of the book also subsequently describes that Chinese urge for untapped resources and new market for generating economic momentum in its landlocked western region or Western Development Strategy encourages China's deeper engagement in South Asia, Central Asia and Middle East. Imperatives of resources and markets drive engagement with Africa and Latin America too, where cultural forays till now are less conspicuous than economic engagement. While both culture and economics, along with public diplomacy, are visible in Southeast Asia, culture dominates other forms of engagement in Northeast Asia and even in USA, Canada and Latin America as these countries do not offer room for strategic gains through economic aid and investment in infrastructure. Specific regional and multilateral imperatives such as recognition of Taiwan and support in the United Nations also drive the engagement with the Pacific Island countries. While writing on so many regions and countries, some of the regions like, such as Oceania, South Pacific, Central Asia, Mongolia lack extensive analysis and other regions, e.g., South Asia and Southeast Asia get rigorous analysis of the various initiatives of Chinese government. In addition, few regions, e.g., Africa and Southeast Asia end with a conclusion on the challenges, successes and failures in terms of leveraging soft power initiatives in the conduct of Chinese foreign policy. Qualitatively, equal analysis of China's soft power initiatives in different regions, its challenges, successes and failures could add value to the book.

In order to compare China's soft power strategies with India, the book reflects on India too. It highlights India's rich endowment of captive soft power stemming from ancient history, civilization, assimilative and cosmopolitan culture, democratic institutions and religious plurality. Although India's soft power efforts have been limited and less conspicuous compared to its larger eastern neighbour, under Modi government Indian foreign policy is increasingly adopting soft power tools. Under two sub-heading 'State-driven Initiatives' and 'Non-state-driven Initiatives' chapter nine goes on to explain different soft

power tools, e.g., cultural initiatives; Buddhism; public diplomacy (viz. social media, Bollywood; TV channels; food; cricket; connecting to diaspora and high level visits) and economic initiatives (viz. regional connectivity, offering aid for infrastructure building and humanitarian assistance). Of these tools, culture has been employed as an important tool of soft power. The author, however, emphasizes on India's foreign policy, particularly the thrust on highlighting cultural virtues in articulating soft power can be somewhat a risky approach to adopt, given that aggressive emphasis on culture and civilization might give birth to fear of cultural colonization among the recipients. It also brings to the fore an explanation on the core strategic objectives, e.g., maintaining a benign external environment; facilitating peaceful conditions for economic growth; advancing its ambition of being a major global or regional power and correcting negative impression of Indian state ability to effectively govern and deliver a decent quality of life to its people that Indian soft power is meant to achieve. Though Parama highlights India's soft power across various regions, India's soft power initiatives in different regions could be broadly explained as the latter part of the book's title implies "Comparative Indian Initiatives".

The book also highlights the Sino-Indian bilateral engagement. While the two countries have been resorting to soft engagement with the rest of the world, such engagement is not exclusive of each other and has been growing in recent years. It shows that robust economic ties and enhanced people-to-people contact through historical linkages like Buddhism and new connection created by state and non-state initiatives in culture and education are establishing the foundation for wider and deeper bilateral engagement. Of different tools of soft power, trade has been the biggest driver of bilateral economic engagement. During the last decade, China became India's largest merchandise trade partner, while India also became one of China's top10 trade partners. However, this perspective on engagement must note an aspect that India is yet to figure as high in China's priorities as China does in India's. By analysing Sino-Indian engagement, an extremely relevant contribution of the book is to trace out the persistence of contradictory position over several issues, e.g., border dispute; India's non-commitment to Belt and Road Initiative (BRI); China's intention to accommodate Bangladesh-China-India-Myanmar Forum for Regional Cooperation (BCIM) within BRI; China's ethnic heterodoxy and chaotic democracy; competitive outlook towards each other; trade imbalance and visa policy between China and India that creates hindrance in their deployment of soft power with respect to each other. It reflects that Chinese interest in contemporary India has increased manifold due to Bollywood films and music, Indian accomplishments in Yoga and IT. On the other hand, Indian younger generations are displaying a more open and receptive attitude towards China, which is evident from the rising number of Indian students in China as well as a steady increase in inflows of tourists. The book goes on to analyze the changing perception of India and China with regard

to each other and the growing pattern of constructive engagement between the two through the application of various soft power tools. But a brief analysis on whether the sense of pragmatic collaboration and the emphasis on constructive engagement through greater use of soft power creates more benign impressions on both sides by denting the trust deficient could enrich the book.

In order to compare China's soft power strategies with India, the author argues India's soft power efforts have been limited and less conspicuous compared to China. To establish this argument author gives two structural differences between India and China's soft power. Firstly, whether it is culture or economic engagement, China is engaging with the rest of the world through soft power on a much bigger scale and faster pace than India. In this regard, author gives an example of India and China's efforts to capitalize soft power through education. Among major Asian countries, India has only nine universities figuring among Asian top one hundred compared with twenty-one from China. Secondly, the difference in scale, pace and intensity between soft power strategies of China and India are also attributable to the degree of involvement of the state in exercising soft power. India has been happy to allow its non-state actors to be more proactive in advancing its soft power. In contrast, China's soft power initiatives are state-driven.

In line with the former argument the author also argues that India's soft power will continue to encounter formidable challenges than China. To strengthen this argument, author identifies several challenges of India's soft power, e.g., religious pluralism; multilingual and multiethnic features; resource constraints; adverse impression over Indian's state inability to provide better quality of lives to its majorities; ineffective communication with the rest of the world and incoherent coercive diplomacy with neighbours like Pakistan. In contrast with India, author also identifies some challenges of China's soft power, e.g., local resentment in Africa, Asia and Latin America, hard postures in the South China Sea and ambiguous postures in the Middle East. It argues, unlike India, China's soft power will not encounter such challenges. In this respect, it also gives an interesting comparison of India's soft power challenges with respect to China's soft power, such as, due to the multilingual and multiethnic feature of India no language of India has attracted as much global attention and inclination to learn as Mandarin has. As China's soft power analysis is the main objective of the book, thus more emphasis on the challenges of China rather than India might enrich it more.

The book also attempts to assess the strategic dividends of China's soft power. It mentioned about different opinion surveys that point to its increasing recognition by the global community. But these opinion surveys might not reveal the true picture, given that positive perceptions do coexist with negative ones.

Therefore, it highlights the adverse impressions range from discomfort over the high cost of Chinese development assistance and indebtedness to China, China's businesses displacing local jobs and livelihoods, Chinese investments being primarily resource-seeking in Southeast Asia, Africa and Latin America. The author is skeptical about whether political and strategic support for major initiatives such as the BRI and the AIIB, expanding a territorial agenda in the South China Sea or containing many countries from diplomatically recognizing Taiwan necessarily imply a 'benign' perception of China. With skepticism, author opines that if it is indeed so, then more than soft, it is approximately smart power that is earning strategic capitals.

The book is thematically well-organized, rich in information and empirical evidence and is also written in a reader-friendly style. As far as the objectives are concerned, the book is a commendable initiative. The title of the book is also consistent with the basic ideas, argument and subject. The rich historiographical account of the book including Kong Zi; Confucius; Mencius; Loa Zi; Zhuang Zi; Sun Zi; Shaohua Hu; Xiang Shu Yong; Zhao Chang Rong; Kautilya; Kamandak; Rabindranath Tagore as well as many scholarly references from E.H. Carr; Joseph Nye; David Leheny; Gallarotti and Gramsci; Habermas will help politician, policymaker, academician, researcher in international relations, political science, non-traditional security studies and other related disciplines of social sciences to understand soft power discourse from a non-western perspective or Asian perspective. The book will, no doubt, have significant contribution to the existing literatures on soft power, China and India's soft power strategies and foreign policies.

The book is not without its limitation. Considering editorial mistakes there are a few spelling and grammatical errors that should be revised in its second edition. The main criticism lies in conceptual stance exclusively. Though, the book is focused on China's soft power it also asserts that China's soft power co-exists with hard power. To justify this assertion, author gives the example of Asia-pacific, Southeast Asia and USA where China's nuanced engagement has been marked by a combination of hard and soft power strategies. It further argues that China's both active employment of soft and hard power might be interpreted as an effective demonstration of smart power. In this respect, chapter one of the book could consider providing some accounts of the concept of hard power and smart power relating to the soft power discourse. Further, an intense discussion about the prospects and strategic outcome of Chinese soft power could ameliorate the book more.

Finally, *Analysing China's Soft Power Strategy and Comparative Indian Initiatives* is an important contribution in the discourse of soft power as it marks several exceptions compared to the prevailing perspectives. For instance,

in contrast with the western academic discourse on soft power, this book conceptualizes soft power from non-western and Asian perspective. The book, by de-Americanizing the concept of soft power, is a significant contribution to the contemporary discourse of soft power in international relations discipline. Likewise, it also adds value to the study of China's soft power as there is lack of focused attention on modern China's extensive deployment of soft power.

Reviewed by
Syeda Tanzia Sultana
Research Officer
Bangladesh Institute of International and Strategic Studies (BIISS)

BIISS Publications

- **BIISS Journal (Quarterly)**
- **Bangladesh Foreign Policy Survey (Quarterly)**
- **BIISS Papers (Monograph series)**
  The Assam Tangle : Outlook for the Future (1984)
  The Crisis in Lebanon: Multi-dimensional Aspects and Outlook for the Future (1985)
  India's Policy Fundamentals, Neighbours and Post-Indira Developments (1985)
  Strategic Aspects of Indo-Sri Lanka Relations (1986)
  Indo-Bangladesh Common Rivers and Water Diplomacy (1986)
  Gulf War : The Issues Revisited (1987)
  The SAARC in Progress : A Hesitant Course of South Asian Transition (1988)
  Post-Brezhnev Soviet Policy Towards the Third World (1988)
  Changing Faces of Socialism (1989)
  Sino-Indian Quest for Rapprochement: Implications for South Asia (1989)
  Intifada : The New Dimension to Palestinian Struggle (1990)
  Bangladesh : Towards National Consensus (in Bangla, 1990)
  Environmental Challenges to Bangladesh (1991)
  The Gulf War and the New World Order : Implication for the Third World (1992)
  Challenges of Governance in India : Fundamentals under Threat (1995)
  Bangladesh in United Nations Peacekeeping Operations (1998)
  Nuclearisation of South Asia : Challenges and Options for Bangladesh (1998)
  The Middle East Peace Process and the Palestinian Statehood (2000)
  Pakistan and Bangladesh : From Conflict to Cooperation (2003)
  Integrated Coastal Zone Management in Bangladesh : A Case for People's Management (2003)
  WTO Dispute Settlement System and Developing Countries: A Neorealist Critique (2004)
  State Sovereignty and Humanitarian Intervention : Does One Negate the Other? (2006)
  Unipolarity and Weak States: The Case of Bangladesh (2009)
  Japan's Strategic Rise (2010)
  The Fallacy of Fragile States Indices: Is There a 'Fragility Trap'? (2017)
- **BIISS Seminar Proceedings**
  Contemporary Development Debate: Bangladesh in the Global Context
  Moving from MDGs to SDGs: Bangladesh Experience and Expectation
  SAARC at 30: Achievements, Potentials and Challenges
  Bangladesh's Relations with Latin American Countries: Unlocking Potentials
  Civil-Military Relations in Democracy: An Effective Framework
  Recent Extremist Violence in Bangladesh: Response Options
  25 March – Gonohottya Dibosh (Genocide Day)
  Reconciling Divided Societies, Building Democracy and Good Governance: Lessons from Sri Lanka
  Promoting Cultural Diversity of Small Ethnic Groups in Bangladesh
  Upcoming 45th Session of the Council of Foreign Ministers of OIC, Dhaka: Revisiting A Shared Journey
  রোহিঙ্গা সংকটঃ বাংলাদেশ কর্তৃক গৃহীত পদক্ষেপ ও পর্যালোচনা
  (Rohingya Crisis: Measures Taken by Bangladesh and An Appraisal)
  Bangladesh Delta Plan 2100
- **BIISS Country Lecture Series**
  BIISS Country Lecture Series: Part- 1
  BIISS Country Lecture Series: Part- 2

BIISS Publications

- **Books**

South Asian Regional Cooperation: A Socio–economic Approach to Peace and Stability
Nation Building in Bangladesh: Retrospect and Prospect
The Indian Ocean as a Zone of Peace
The Security of Small States
ASEAN Experiences of Regional and Inter-regional Cooperation: Relevance for SAARC
Development, Politics and Security: Third World Context
Bangladesh and SAARC: Issues, Perspectives and Outlook
Bangladesh: Society, Polity and Economy
South Asia's Security: Primacy of Internal Dimension
Chandabaji Versus Entrepreneurship: Youth Force in Bangladesh
Development Cooperation at the Dawn of the Twenty First Century: Bangladesh-German Partnership in Perspective
Conflict Management and Sub-regional Co-operation in ASEAN: Relevance of SAARC
National Security of Bangladesh in the 21st Century
Civil Society and Democracy in Bangladesh
Regional Co-operation in South Asia: New Dimensions and Perspectives
Confidence Building Measures and Security Cooperation in South Asia: Challenges in the New Century
Bangladesh-Southeast Asia Relations: Some Insights
Security in the Twenty First Century: A Bangladesh Perspective
25 Years of BIISS: An Anthology
Politics and Security in South Asia: Salience of Religion and Culture
Small States and Regional Stability in South Asia
Religious Militancy and Security in South Asia
Global War on Terror: Bangladesh Perspective
Towards BIMSTEC-Japan Comprehensive Economic Cooperation: Bangladesh Perspective
Democracy, Governance and Security Reforms: Bangladesh Context
Whither National Security Bangladesh 2007
National Security Bangladesh 2008
Human Security Approach to Counter Extremism in South Asia: Relevance of Japanese Culture
National Security Bangladesh 2009
Energy Security in South Asia Plus: Relevance of Japanese Experience
Changing Global Dynamics: Bangladesh Foreign Policy

South Asia Human Security Series:

Nepali State, Society and Human Security: An Infinite Discourse
Evolving Security Discourse in Sri Lanka: From National Security to Human Security
Violence, Terrorism and Human Security in South Asia
Women and Human Security in South Asia: The Cases of Bangladesh and Pakistan
Human Security in India: Health, Shelter and Marginalisation
Pakistan: Haunting Shadows of Human Security
Human Security in India: Discourse, Practices and Policy Implications
Human Security Index for South Asia: Exploring Relevant Issues
Ethnicity and Human Security in Bangladesh and Pakistan