JINNAH INSTITUTE

POLICY BRIEF

June 20, 2018

STRATEGIC SECURITY INITIATIVE

In this Issue

Terrorism in the age of New Media

By Meera Nadeem

Terrorism in the Age of New Media and Information Technology, where Conventional Threats to Global Security Meet the Contemporary

Introduction

In an age of connectivity and increasingly porous national borders, threats to global security transcend limitations imposed by geography and conventional application of force. The realm of new media provides a space for violent non-state actors to employ non-traditional tools for narrative building, propaganda and recruitment to their ranks unrestricted by geography or operational capabilities. This imposes new security challenges to the world, with an increased impact on existing human, resource and national insecurities. At the moment, the global response to this very imminent threat has been both inefficient, ineffective, and uncoordinated - with a significant gap in capabilities between countries that are leaders in information technology and those that bear the brunt of terrorist violence.

This paper will examine the use of new media tools by modern violent extremist groups to build their narrative and develop self-sustaining "online" networks that allow them to increasingly impact the global information environment, and maintain adaptive terrorist networks. The paper will also review existing mechanisms being employed to counter these extremist ideologies within cyber terrorism, and identify the gaps that exist between the two, proposing possible policy measures and robust cross-disciplinary implementation strategies as a sustainable way forward towards ensuring global security and peace in the 21st Century.

What is New Media?

New media includes mass communication platforms that allow for two-way interaction between user and consumer, and differ from traditional and conventional media in many respects such as interactivity, reach, frequency, usability, immediacy and permanence. Commonly, these are referred to as social media platforms, the most popular of which include Facebook, Twitter, YouTube, and Instagram. Unlike traditional media and its one-to-many approach where only a small cohort of established, regulated institutions disseminate information to an effectively limitless audience, social media enables two-way communication in which the information consumers also act as the communicators.

A far more important factor that differentiates new media outlets from traditional media is the control and regulation that is associated with it, or lack thereof. While traditional media outlets such as TV, radio, and newspapers undergo a strict editing and vetting process, usually regulated by the state, social media platforms evade such regulations and censorship altogether.

These modern communication technologies have increasingly become popular with terrorists and violent extremists, particularly new media platforms that enable real time interaction between user and audience. These are useful for terrorists in that there is less transmission time involved, immediate feedback loops, significantly low costs of communication, and integration communication that leads to the sustainable dissemination of information. Terrorist organisations are increasingly employing strategies of utilising interactive social media tools to bring together like minded people to increase radicalism, particularly targeting the younger generation who have essentially grown up watching youtube vistas, and for whom social media has become an integral part of life.

Modern Violent Extremism and the Internet

According to a UN agency that oversees international communications, and Time magazine, over 4 billion people are using the Internet today; that is over half of the world's total population. Social media use is also rapidly growing, with over 3 billion people around the world using it each month, 9/10 of whom access their chosen platforms via mobile devices. The implications of this immediate access to information are crucial, and the biggest advantage modern violent extremist groups have to their cause today. This means that these social media platforms are not only user friendly, but also give terrorists direct "door access" to their target audience, as opposed to traditional media outlets and the Internet 1.0 where the use of websites involves the consumer visiting the website, and not vice versa. Here, we can classify these websites as the Internet 1.0, while the advent of social media where user-consumer interaction was enabled can be classified as the Internet 2.0. It is also important here to differentiate between cyber-warfare and cyber terrorism, where the former includes attacks on computer networks, including those on the Internet itself, while the latter involves the smart use of the Internet by terrorists as a vehicle through which to launch an attack. Terrorists could also conceivably hack into electrical grids and security systems, or perhaps distribute a powerful computer virus.

Terrorism on the Internet is dynamic as websites emerge suddenly, terrorists frequently modify their formats, then swiftly disappear, or in many cases only temporarily disappear by changing their online address while retaining the same content. Ease of access to the Internet, little or no regulation or censorship by the government, potentially huge audiences spread throughout the world, anonymity, fast flow of information and immediately established feedback loops, inexpensive development and maintenance of web presence, dissemination through multiple mediums, and the ability to shape coverage in traditional mass media are all benefits accrued by violent non-state actors in their use of new media platforms. These tools provide terrorists the space to build their narrative and develop self-sustaining "online" networks that allow them to increasingly impact the global information environment, and maintain adaptive terrorist networks. Professor of Defense Analysis at the Naval Postgraduate School California, John Arquilla identifies "stealth" as the greatest advantage of the Internet to terrorists where they "swim in an ocean of bits and bytes," having developed sophisticated encryption tools and creative techniques that make the Internet an efficient and relatively secure means of correspondence. These include steganography, a technique used to hide messages in graphic files, and "dead dropping" transmitting information through saved email drafts in an online email account accessible to anyone with the password.

The use of the Internet by terrorists is not new. Soon after the September 11 attacks and the antiterrorism campaign that followed, a large number of terrorists moved to cyberspace, setting up thousands of websites that promoted their messages and activities. However, many of these were shut down by intelligence agencies and anti-terror activists who monitored the sites, attacked some of them and forced their operators to seek new online alternatives. This marked the shift of terrorist's use from the Internet 1.0 to the Internet 2.0. By the year 2000, virtually all proscribed terrorist networks had an established Internet presence.

As Evan Kohlmann argues, today, 90 percent of terrorist activity on the Internet takes place using social networking tools. These forums act as a virtual firewall to help safeguard the identities of those who participate, and they offer subscribers a chance to make direct contact with terrorist representatives, to ask questions, and even to contribute and help out what he calls "cyber-jihad". Moreover, Gabriel Weimann's extensive research on the topic finds that about 90 percent of organised terrorism on the Internet takes place via social media. It is important to note that the use of social media is not only limited to spread its message and recruit followers, but also to empower its supporters to take part in the same process, an enabling tool that traditional internet 1.0 forums previously lacked.

How Do Terrorists (mis)use the Internet?

It is by and large the case now that the architects of terrorism exploit the media for the benefit of their operational efficiency, information gathering, recruitment, fundraising, and propaganda schemes. Their aim is to publicise their political cause through the media, inform both friends and foes about their motives for terrorism and explain their rationale for resorting to violence. Their target audience includes current and potential supporters as recruits, such as seen in the recent launch of the Tehrik-e-Taliban Pakistan (TTP)'s english-medium women's magazine Sunnat-e-Kahula, that targets young, educated modern women to join their ranks; international public opinion, i.e. the international public who are not directly involved in conflict but have some interest in the issues involved, are courted with sites in multiple languages. Traditional media is also seemingly targeted as an information consumer as evidenced by ready to publish press releases, as well as detailed background information that is useful for international reporters such as Hezbollah's websites that specifically address journalists, inviting them to interact with the organisation's press office via email; and lastly, enemy publics that can be defined as the citizens of states against which the terrorists are fighting or targeting, this too is evident in the efforts of stimulating public debates to change public opinion and weaken public support for governing regimes. These terrorist networks use Internet demographics to narrow down and identify their target audience, from personal information that is usually pulled from online questionnaires and order forms.

In a United States Institute for Peace report, Gabriel Weimann identifies at least eight ways in which modern violent extremists use the Internet to advance their cause, ranging from psychological warfare and propaganda to highly instrumental uses such as networking, fundraising, recruitment, data mining, and coordination of actions.

Terrorism itself is a form of **psychological warfare**, and with the sophisticated use of the Internet, modern violent extremist groups have sought to do so by campaigning though the Internet. This can be done in several ways: by spreading disinformation, to deliver threats that are decentralised or untraceable, to instil fear and helplessness in their audience and the masses, to disseminate their message and activity to the world, a classic current example of which is ISIS/Daesh and their high production value videos of beheadings, designed to spread fear in their audience. Continued psychological warfare is also done through cyberterrorism or cyber-fear, i.e. threats generated about cyber-attacks such as disrupting national economies by hacking computer systems that regulate stock markets or government databases, threats of

disabling airlines by disabling air traffic controllers, etc, all of which are done by hacking and wrecking the computerised systems of world economies.

Until the advent of the Internet, non-state actors and terrorists had limited outreach to secure **publicity and spread propaganda** with mediums like TV, radio and print media, all of which were regulated and controlled by the state. With the Internet and social media however, these groups now have direct and almost complete control over the content of their messaging and its dissemination which allows them to further shape and manipulate their target audiences as well as their own image, and also cash in on Western sympathy from those who lobby for freedom of expression. As a consequence, they also now hold the power to influence what news content traditional media carries.

According to Dan Verton in his booked titled Black Ice: The Invisible Threat of Cyberterrorism (2003), Al-Qaeda cells now operate with the assistance of large databases containing details of potential targets in the US - this is done by **data mining** and **information sharing**, i.e. the harvesting and collection of intelligence on those targets, especially critical economic nodes, with the help of modern software. Important information is sought out by sophisticated terrorist outfits as well as by individuals to use these to advance their own agendas, including how to access data and how to manufacture explosive devices. Numerous tools are available to facilitate such data collection, including search engines, email distribution lists, chat rooms, and discussion forums. A website operated by a Muslim hacker group called the Muslim Hackers Club that develops software tools to launch cyber-attacks has also featured links to US sites that purport to disclose sensitive information such as code names and radio frequencies used by the US Secret Service. This website is just one example of such a platform that offers tutorials for creating and spreading malware and viruses, devising hacking stratagems, sabotaging networks, and developing codes; it also provides likes to other militant Islamic and terrorist web addresses.

Like any other political organisation, terrorist groups also use the Internet for **fundraising and acquiring weapons.** Many of these groups such as Al-Qaeda and Daesh heavily depend on donations, with heir global fundraising networks built upon a foundation of charities, NGOs, and other financial institutions that use websites and the Internet for their gains. The Hizb-ul-Tahrir is another example of a terrorist group that uses integrated websites with outreach and support from Europe and Africa, asking their supporters to assist their cause and make donations. Similarly, the illegal sale and purchase of heavy weapons, guns and ammunition are also made on social media platforms such as Facebook, as evidenced by a recent report by the First Post, where it was reported that active terror groups in Syria were using Facebook to purchase ammunition, and heavy weapons such as MANPADs, a type of anti-aircraft missile launchers that are one-man-portable air defence systems were on sale on the social media platform. The ease with with these weapons are openly available and advertised means these can easily fall into the wrong hands, and therefore poses a grave security risk to the world.

Beyond soliciting donations from sympathisers, the Internet is also used for **recruitment and mobilisation** of supporters to play a more active role in support of terrorist activities or causes. Electronic bulletin boards and user nets also serve as vehicles for reaching out to potential recruits, while inversely, would-be-recruits also use it to reach out to and offer themselves to terrorist organisations. The SUTE Institute, a Washington based terrorism reproach group that monitors Al-Qaeda's internet communications has provided chilling details of a high-tech recruitment drive launched in 2003 to recruit fighters to travel to Iraq and attack the US and coalition forces based there. This aspect of the use of the Internet by terrorist groups goes hand in hand with **establishing networks** between loosely interconnected groups, that are increasingly able to maintain contact with one another in a more decentralised and untraceable manner.

Terrorists use the Internet not only to manufacture strategies and attacks, but also for **planning and coordination for activities** and for the mobilisation of large groups. Al-Qaeda's use of the Internet to coordinate and plan the September 11 attacks is a prime example of such planned coordination, where thousands of encrypted messages were later found by federal officials on the computer of the arrested mastermind. Online platforms used to promote electronic jihad are also used for operational purposes such as instruction and training, such as the 2008 Mumbai bombings, where numerous attacks in scattered locations through the city were executed by terrorists who used advanced communication technologies including handheld GPS devices to plan and execute their attacks, Google Earth satellite imagery and live updates shared on mobile phone devices to monitor their hostages and update their handlers. In a detailed report for the Willson Centre, Gabriel Weimann states that these postmodern terrorists use a variety of new social media platforms to direct their followers to websites with instructional material, promoting hacking techniques and sharing encryption programs that include instructional YouTube videos and Facebook posts to teach the use of explosives, and train in virtual online camps.

Imminent threat today: ISIS/Daesh

Steven Stalinksy and R. Sosnow (2015) find that the Islamic State of Iraq and Syria (ISIS) and Daesh posit a direct threat to international safety and security today, as it is the largest in land control and fighting size, as well as the wealthiest terrorist organisation in history. Prior to the military crackdown against it, ISIS controlled more territory and rescuers than any terrorist organisation that has ever existed. According to a Brookings Institute study, the organisation has expanded its influence well beyond the battlefield, with amateur videos and images being uploaded daily by its foot-soldiers, that are then globally shared both by ordinary users and mainstream news organisations. In many aspects, ISIS has learned its propaganda from Al-Qaeda, however it has quickly overtaken its mentor in deploying a range of narratives, images, and political proselytising through various social media platforms. Testifying before the US House of Representatives Committee on Foreign Affairs in 2015, J.M. Berger said that as of 2014, there were at least 45000 Twitter accounts used by ISIS supporters, many of which have by now been suspended. With their sophisticated use of the Internet and social media, we have seen the rise of a highly organised social media campaign that uses deceptive tactics and reflects a sophisticated understanding of how such networks operate.

With their carefully crafted recruiting pitches, ISIS uses stirring imagery in professionally produced videos with what is mostly welcoming content in tone and tenor, designed to expertly target real or imagined ambitions and grievances, appealing to potential recruits' emotionally and religiously charged sense of adventure, offering an attractive cause worth fighting for. These pitches are especially designed to elicit sympathy and support for a virtually connected community of ISIS fans and followers, and creates an echo chamber of reinforcement of what ISIS stands for, that is to fight for social justice and protect Muslims in an unfair global system, says John Graham in his research on the extremist group.

Today, ISIS is continuing to successfully attract recruits from around the world, where many young would-be jihadis travel to Iraq and Syria to fight, while others come to be trained in terrorist tactics that they can employ upon return to their own homelands. Other extremists-in-training do not leave their homelands at all, but are continuing to be indoctrinated over the Internet to do jihad in their own communities. What is more alarming is that despite escalating losses in Syria and Iraq, the ability of ISIS to continue to carry out and inspire attacks far beyond these countries remains successful. According to a 2016 study for the National Bureau of Economic Research, Tunisia, Saudi Arabia, Russia, Turkey, and Jordan are the top five countries that ISIS recruits its foreign fighters from.

The rise of online terrorism is also increasingly inspiring isolated acts of terrorism both online and offline, as evidenced by the case of the Orlando nightclub shooting of 2016. Lone wolf acts of violence and terrorism are becoming rampant, and is reportedly the fastest growing kind of terrorism particularly in the West, where the terrorists are individuals who are radicalised, recruited, trained, and even launched on social media platforms.

Existing Counter Mechanisms to Cyberterrorism and their Failures

While mass media, policymakers, and security agencies tend to focus on the exaggerated threat of cyber terrorism, they pay insufficient attention to the more routine uses of the Internet which are seemingly numerous, and from the point of view of terrorists, invaluable. Although strict counterterrorism measures will help defend our increasingly tech-reliant societies against cyberterrorism, these also present serious challenges such as more authoritarian, Orwellian governments and agencies with little public accountability tools. This in turn results in privacy violations, curtailed flows of public information, restricted freedom of expression and censorship that ultimately results in diminished civil liberties, the long term implications of which could be profound and damaging for democracies and the values they stand for. It is therefore imperative to remain mindful of the fact that the use of advanced techniques to monitor, search, track, and analyse communications holds inherent dangers.

Today, terrorists have turned to new media not only because counterterrorism agencies have disrupted their traditional online presence, but also because new media offers them far more benefits than traditional media for information dissemination. According to the European Council on Foreign Relations, to date, the dominant approach pushed by European policy-makers and companies alike is to focus on the restriction and removal of content on the Internet in order to contain the spread of extremists' messaging efforts. While the National Security Agency, the Department of Defense, the CIA, the FBI, the Defense Intelligence Agency, other US and foreign intelligence agencies, and some private contractors are already fighting back, monitoring suspicious websites and social media, cyber-attacking others and planting bogus information, the virtual war between terrorists and counterterrorism forces remains ferocious. More recently, the UK and France have also agreed to launch a bilateral camp to tackle online radicalisation by imposing fines on tech companies that fail to remove extremist content.

However, such measures have also met strong criticism as noted by Peter Neumann, Director of the International Centre for the Study of Radicalisation in his talk on online radicalisation, where he states that censorship only serves as a minor disruption to online activities of terrorists and extremists, but it does not eliminate them. This is also evidenced by a New York Times report which highlights the suspension of over 200 thousand extremist accounts in 2016 that led to the widespread migration of extremist content from open or public platforms, to end-to-end encrypted messaging services such as WhatsApp, thereby making it more difficult for law enforcement agencies to monitor their activities.

Shutting down a terrorist website only serves as a temporary disruption. In a publication of the Council of Foreign Relations, Eben Kaplan finds that the ability of the US National Security Agency to monitor such individuals inside the United States has been the subject of a heated political and legal debate. The United States has tried to prosecute webmasters who run terrorist websites in the West, but has run into opposition from advocates of free speech. Defense analyst and Professor John Arquilla also posits that "sites that tell the terrorist side of the story go right up to the brink of civil liberties." Sami Omar al-Hussayen, a Saudi Arabian graduate student at the University of Idaho, was charged by U.S. officials with supporting terrorism because he served as a webmaster for several Islamic groups whose sites linked to organisations praising terrorist attacks in Chechnya and Israel. Al-Hussayen was acquitted of

all terrorism charges by a federal court in June 2004 under the First Amendment. Two months later, Babar Ahmad, a 31-year-old, British-born son of Pakistani immigrants, was arrested in London under a U.S. warrant.

According to The White House counter-radicalization strategy published in August 2011, the importance and role of the Internet and social media in advancing violent extremist narratives is largely recognised. While the implementation plan itself outlined new programs and initiatives, and committed the then US administration to formulate a strategy in its own right whereby it would develop a separate and more focused comprehensive strategy for countering and preventing online violent extremism and radicalization, as well as a strategy for the leveraging of technology to empower community resilience, no such online strategy has been formed so far.

Possible Policy Measures to Ensure Sustainable Global Security and Peace

According to the Countering Online Radicalization in America report which identifies shortcomings in the US online counter-radicalization strategy, approaches aimed at restricting freedom of speech and removing content from the Internet are not only the least desirable, but also the least effective. Instead, it recommends that the government should play a more energetic role in reducing the demand for radicalization and violent extremist messages.

Despite the rapid growth of information technology and internet research, including the Internet itself, efficient strategies or fruitful countermeasures to cyber terrorism have not yet been provided, and there remains a significant gap between the two. A deeper understanding is required about modern violent extremism and terrorism, particularly with the smart use of the Internet, the deep web and social media, and new types of online warfare, intelligence gathering and training for cyber armies are the need of the day. A threat that emerges in one corner of the world is no longer restricted to that area by geography; the Internet and social media have allowed for the world to become a 'glocal' place, with one act of terrorism potentially threatening the entire world on an exponential scale.

Cyberspace, with its numerous and emerging online platforms, presents new challenges to global security and requires dramatic shifts in strategic thinking regarding national and global security, and countering terrorism. Military operations against terrorism should be led by companies bound together by a digital communications strategy that provides audiovisual material that can be shared on social media. Strategic thinkers should look beyond current challenges to future developments and emerging social media resources, and the problems of anticipating and preempting terrorist abuse of these tools.

References

1. Benmelech, Efraim & F. Klor, Esteban (2016, April) What Explains the Flow of Foreign Fighters to ISIS? National Bureau of Economic Research http://www.nber.org/papers/w22190

2. Berger, J.M. (2015, January 25). The Evolution of Terrorist Propaganda: The Paris Attack and Social Media, *Brookings Institute* https://www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/

3. Davidson, Jacob. (2015, May 26). Here's How Many Internet Users There Are, *Time* http://time.com/money/3896219/internet-users-worldwide/
4. Elgot, Jessica (2017, June 12). May and Macron plan joint crackdown on online terror, *The Guardian* https://www.theguardian.com/politics/2017/jun/12/may-macron-online-terror-radicalisation

5. Graham, John. Who Joins ISIS and Why? *The Huffington Post* https://www.huffingtonpost.com/john-graham/who-joins-isis-and-why_b_8881810.html

6. Homeland Security Project, Countering Online Radicalization in America (2012, December), *Bipartisan Policy Center* http://bipartisanpolicy.org/sites/default/files/BPC%20_Online%20Radicalization%20Report.pdf

7. Idahosa, Stephen. (2017). International Terrorism: The Influence of Social Media in Perspective, *World Wide Journal of Multidisciplinary Research and Development.* 3. 86-91. https://wwjmrd.com/upload/1509043009.pdf

8. Islamic State, Al-Qaeda using social media to buy weapons: Report (2016, February 25), *First Post* https://www.firstpost.com/india/islamic-state-al-qaeda-using-social-media-to-buy-weapons-report-2643386.html

9. The Islamic State: Background, *The Jewish Virtual Library* www.jewishvirtuallibrary.org/jsource/Terrorism/ISISback.html

10. Kaplan, Eben. (2009, January 8). Terrorists and the Internet, *Council on Foreign Relations* https://www.cfr.org/backgrounder/terrorists-and-internet

11. Kemp, Simon. (2018, January 30). Digital In 2018: World's Internet Users Pass the 4 billion mark, *We Are Social* https://wearesocial.com/blog/2018/01/global-digital-report-2018

12. Nadeem, Meera. (2017, August 10). Women in the TTP: Recruiting Across the Gender Divide, *The Express Tribune* https://tribune.com.pk/story/1477711/women-ttp-recruiting-across-gender-divide/

13. Newmann, Peter. Online Radicalisation – Myths and Reality (2017), *Republia* https://re-publica.com/en/session/online-radicalisation-myths-and-reality

14. Poe, Ted. (2015, February 26). Time to silence terrorists on social media, *CNN* https://edition.cnn.com/2015/02/25/opinion/poe-terrorism-social-media/index.html

15. Soesanto, Stefan & D'Incau, Fosca (2017, July 19). Countering Digital Radicalisation, *European Council on Foreign Relations* http://www.ecfr.eu/article/commentary_countering_digital_radicalisation_7216

16. Tracking Terrorists Online (2006, April 19), *Washington Post* http://www.washingtonpost.com/wp-dyn/content/discussion/2006/04/11/DI2006041100626.html

17. Twitter suspends 235000 more accounts over extremism (2016, August 19), *The New York Times* https://www.nytimes.com/2016/08/19/technology/twitter-suspends-accounts-extremism.html?mtrref=www.ecfr.eu&gwh=0DC6AE6C592B65D04B902D720A95F897&gwt=pay

18. Verton, D. (2003). Black ice: The invisible threat of cyber-terrorism. New York: McGraw-Hill/Osborne.

http://www.worldcat.org/title/black-ice-the-invisible-threat-of-cyber-terrorism/oclc/52907324

19. Weimann, Gabriel. (2004) How Modern Terrorism Uses the Internet, *USIP* https://www.usip.org/sites/default/files/sr116.pdf

20. Weimann, Gabriel. (2014). New Terrorism and New Media. *Willson Center* https://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F_0.pdf

21. Weimann, Gabriel (2014, February 25). Virtual Packs of Lone Wolves, *Medium* https://medium.com/p/17b12f8c455a.

22. The White House, (2011, August 6). Empowering Local Partners to Prevent Violent Extremism in the United States, *Department of Homeland Security* https://www.dhs.gov/sites/default/files/publications/empowering_local_partners.pdf

23. The White House, (2011, December 20). Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States, *Department of Homeland Security* https://www.dhs.gov/sites/default/files/publications/empowering_local_partners.pdf