

Challenges to fighting transnational terror networks



**ASSIGN
BUSTER**

Traditional State Power limitation in dealing with Transnational Terror Networks: and the role of Social Media

Governments have been phased with challenging situations when implementing effective counterinsurgency measures against rebel groups that override national boundaries; even despite superior power. For example, the Afghan government and U. S./NATO coalition forces and their inability to defeat Taliban and Al-Qaeda militants, despite their joint and greater vitality (Salehyan, 2009). In the case of the Taliban and Al-Qaeda, rebels we're defying and trouncing government efforts through sanctuaries, surpassing borders, and that of government exercises too. At the time, these groups we're one of the first demonstrations of terror organizations that were not territorially bounded and the implications of such regional mobility.

In today's 21st century, borders have become even more porous. The current globalized world, has reached a new level of interconnectedness. Through technology, the media, and the effects of globalized markets, sovereign statehood, as we once knew it is transforming. The contemporary interconnectedness is dissolving the significance of borders and boundaries once established by the Treaty of Westphalia in 1648. Explicitly, such transformation from the dynamics of globalization has been the advancement of terrorism from a regional phenomenon into a global one.

Social Media, is one of the most critical dynamics of globalization that's contributing to global terrorism. Traditional state power is limited in dealing with transnational terror networks that organize through social media. The United States, serves as an examples of such limitations with its rise of

homegrown extremism despite the state's strong traditional military, economical, and even political power. In a time-span of twelve years since the 9/11 attacks, there was a total of 60 Islamist-terror plots against the United States, and 49 of which were homegrown terror plots inspired through social networks (Bucci, 2013). Homeland security and the intelligence community are being presented with a modern challenge to counterterrorism.

Much like the implications that were brought upon the Afghan government and the U. S./NATO coalitions forces, from the trans-border Al Qaeda and Taliban sanctuaries, social media is providing a global nexus of sanctuaries for terrorist networks.

Whereas in the past, these transborder dynamics were difficult to contain within national boundaries, terrorists have now gained the ability to organize in external sanctuaries with no attachment to a physical location (Salehyan, 2009). Social media, has become a fundamental role in terrorist operational strategy. It's important to note the complexity of social media, as there are thousands of platforms and each caters to very different arrays of people. For example, Instagram caters to the kind of person who best expresses themselves through photographs, versus Twitter accounts for people who communicate through short bursts of information; each form of media, serves a purpose for an audience that the other may not (Hale, 2017). These advancements have given terrorist organizations the ability to attack informally to a much larger audience, at any time or any given location.

Thus, the battle against terrorism is no longer a structured one that can be challenged with military power (Ressler, 2006). Terrorist's exploitation of these technologies into their organizations, is changing the nature of warfare. Markedly, the attacks in London and Sharm-el Sheikh in 2005, were discovered to have been facilitated by training that was available electronically (Forest, 2007). What became one of Egypt's most, deadliest terrorist attacks, in history, was completely conspired, trained, and even instructed through online sources.

Cyberterrorism, is changing the nature of combat, and as a result creating the need for a new type of intelligence, in which traditional power will play a subordinate role. Military power will continue to be undermined through the use of 'internet sanctuaries'. Infiltration of these organizations will not prevail, in the traditional and physical manner; cyber-infiltration is the contemporary power needed to monitor and diffuse terror-net hotspots.

Terrorist's ability to communicate instantly and across great distances is not the only implication exposed. It's their ability to intelligently use these different social platforms to market their ideology, that has also changed the nature of terrorism. The most notable success of this kind of ideological marketing, has been the Islamic State (ISIS), in marketing its caliphate. Through its jihadist influx of propaganda, the Islamic state, has conquered a territory no other organization has before, the world of social media. (Engel, 2015). The terrorist organization has traces in almost every social network including Twitter, Instagram, Pinterest, Facebook, YouTube, as well as multiple presences in the dark web.

The organization's ability to assess the differences between each platform, is evident in their intelligently distinctive approach in propagandas through the varying platforms. Twitter in particular, has been used to drive communications by the jihadist organization. In 2014, there was a collection of 59 Twitter accounts that linked to western-origin fighters known to now be in Syria (Klausen, 2014). The significance of the role of social media on terrorism, is due to the fact that by previous nature, extremists have lacked wide support for their radical ideas, which forced these groups to need to provoke drastic acts to receive attention, and televised response. Terrorism through this aspect was the weakest form of irregular campaigning.

As a result of this new facilitation of transnational communication through social networks, terrorists have gained the ability to reach new targets for recruitment and expansion. The increasingly worldwide perception of Muslim oppressions, is providing organizations like the Islamic State, with direct opportunities of spreading their radical beliefs to the exterior countries, specially in the west. Targeting these sympathizers, whom feel alienated in western societies, by portraying ISIS territory in a very pleasant and welcoming community of the "Muslim brotherhood." Infusing their social-media dominance to their recruiting techniques, the organization has been successful in spreading a western encouragement to migrate to Syria.

Roughly, 4,000 foreigners of ISIS' fighting force have come from western countries (Engel, 2015). Recruiters are targeting minorities and recent Muslim converts, through chatting apps like Kik, to advise these potentials on routes to Syria through Turkey, and even offer recruitment arrangements. With the recent Muslim travel bans by the United States, extremists are further

provoking vulnerability for sympathizers, and providing terrorist with support of caliphate radicalization.

However, although technology has improved the ability for terrorist to work together, and reach a new audience, technology can't change the character of the terrorist message or the nature of struggle (Baylis, 2011). That is, regardless of the new methods, there are still patterns and trends in these organizations' characteristics that are not altering.

The identification of such characteristics for potential perpetrators is of critical importance for the prevention and deterrence of the contemporary nature of terrorism (Dolnik, 2007). Profiling the organization's activities and modifications, gives exhibition to the group's 'modus operandi;' that is a particular way or method of doing something, that's characteristically well-established (Dolnik, 2007). There seems to be a direct correlation between the variables in these organizations' modus operandi, with their group dynamics, including their structure and ultimately their durability. It has been approximated that only one out of ten organizations survive the first year of operations (Dolnik, 2007). Through Dolnik's research, in critical elements of predictive threat assessment from terrorist violence, he identifies the interrelationship between a groups' level of technological innovation and its life-span length. Considering the importance for these organizations to adopt and habituate to technological advances, for their durability, this detail provides contingency for state intervention in a sui generis power that surpasses the traditional limitations.

In spite of the terrorist use of social networks for extremist movements, the publication of their actions and their digital footprint leaves behind opportunity to profile and determine these terror organization's modus operandi. Understanding these extremists' ideologies and strategies is critical, because, it's these ideologies that are ultimately the driving force behind these networks. Knowing what drives them, is knowing how to destruct them. The British intelligence agency, MI5 provides an example of such counterinsurgency success in the 1930's, using the same methods of data fusion to defeat Soviet communist recruitment in Britain. Using a Domestic Signals Intelligence (SIGINT) combined with defensive counterintelligence ops (such as surveillance), the agency was capable of comprehending the underground network, identifying the structure, and its methods for activities. Through this knowledge of how the network was operating, MI5 was able to infiltrate by strategically setting themselves up for recruitment, and ultimately defeating them. The same strategy for data fusion is needed to triumph on the war of cyberterrorism.

Acquiring new techniques that optimize the ability for information systems, to acquire and measure sets of key information within social networks; is the type of data advancement needed to deal with insurgencies that organize themselves through social medias. Already established (SNA) Social Network Analysis, study's the relations, ties, patterns, and communications within social groups (Ortiz-Arroyo, 2009). But the success of defeating these terrorist organizations will come almost directly from the knowledge of its structure, and that will include identifying the sets of key players and their relations within social networks. Discovering such sets of players is based on

entropymeasures, which uses a ' Galois Lattices' mathematical approach of nodes (or actors) and edges (or sets oflinks) to create a map of interaction between the two (Ortiz-Arroyo, 2009). Incorporating these technique of computer analysis into encryptions withfunctionality measures of centrality, which measure certain assumptions aboutthe flow of information in networks, will provide states with greater advantagein defensive counterintelligence. Particularly, in combating and defusingterrorist radical messages in the domestic sector.

State power in combating terror networks is contingent upon adapting to the modern conflicts of terrorism. While the strategy used by the MI5, for data fusion is still valuable, new implications of encryption are needed for the current information revolution. The post 9/11 terror attacks in the United States, was the event that led to the commencement of Intelligence reforms. The Terrorist Prevention Act of 2004, paved the way for important network structure analysis and surveillance systems. However, through reversal of the surveillance act by, domestic counterintelligence has been in great disadvantage to the modern terrorist adversaries.

The modern era of terrorism through networks, provides challenges to traditionalcounterinsurgent techniques. By increasing the role of the private sector inespionage, and surveillance, States can surpass the limitations being presentand avoid the critics of policy that occurred during the 2004 Intelligencereforms. The private sectors, can also assist with using social media to thestates' advantage, by educating the targets whom by the trends can be depicted, and educating the on the risks associated with extremist and social medias.

<https://assignbuster.com/challenges-to-fighting-transnational-terror-networks/>

These domestic limitations are of advantage for adversaries, like ISIS, that can utilize these domestic implications against the state. Improving technology monitoring and analysis, is imperative to overcome the traditional limitations of state power in combating transnational terrorist networks that organize through social networks.

Works Cited:

- Salehyan, I. (2009). *Transnational Insurgencies in World Politics. Rebels without Borders*. doi: 10.7591/9780801459214-toc Cornell University Press
- Bucci, S. (n. d.). 60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism. Retrieved July 28, 2017, from [http://www. heritage. org/terrorism/report/60-terrorist-plots-911-continued-lessons-domestic-counterterrorism](http://www.heritage.org/terrorism/report/60-terrorist-plots-911-continued-lessons-domestic-counterterrorism)
- Hale, B. (2017, February 26). The History of Social Media: Social Networking Evolution! Retrieved July 28, 2017, from [http://historycooperative. org/the-history-of-social-media/](http://historycooperative.org/the-history-of-social-media/)
- Ressler, S. (July 2006). Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research. Retrieved July 26, 2017, from [https://search. proquest. com/docview/1265818456? pq-origsite= gscholar.](https://search.proquest.com/docview/1265818456?pq-origsite=gscholar)
- Forest, J. (2007). *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*. Retrieved from [http://eds. b. ebscohost. com. ezproxy. fiu. edu/ehost/ebookviewer/ebook/bmxlYmtfXzlyNjMyNF9fQU41? sid= 43dc8b2f-6de1-41a7-b2bd-14550103741d@sessionmgr104&vid= 0&format= EB&lpid= lp_a&rid= 0](http://eds.b.ebscohost.com.ezproxy.fiu.edu/ehost/ebookviewer/ebook/bmxlYmtfXzlyNjMyNF9fQU41?sid=43dc8b2f-6de1-41a7-b2bd-14550103741d@sessionmgr104&vid=0&format=EB&lpid=lp_a&rid=0)
- <https://assignbuster.com/challenges-to-fighting-transnational-terror-networks/>

Engel, P. (2015, May 9). ISIS had Mastered a crucial recruiting tactic no terrorist groups has ever conquered. Retrieved from <http://www.businessinsider.com/isis-is-revolutionizing-international-terrorism-2015-5>

Klausen, J. (2014). Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38 (1), 1-22. doi: 10. 1080/1057610x. 2014. 974948

Dolnik, A. (2007). Understanding Terrorist Innovation. *Contemporary Terrorism Studies* . doi: 10. 4324/9780203088944 Technologies, Tactics, and Innovations

Ortiz-Arroyo, D. (2009). Discovering Sets of Key Players in Social Networks. *Computer Communications and Networks Computational Social Network Analysis*, 27-47. doi: 10. 1007/978-1-84882-229-0_2

Baylis. The Globalization of World Politics (John Baylis, Steve Smith, Patricia Owens)