Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

ACTIVIST HACKERS VS ISIS: BATTLING THE PROVERBIAL FRANKENSTEIN MONSTER IN CYBERSPACE

Gp Capt Ashish gupta
Senior Fellow, CAPS

Terrorism - a scourge that transcends the geographical borders and cuts across religious, sectarian and ethnic lines- evolves, propagates and retains its terror potency by permeating the public consciousness and infesting our societies with fear. The degree of success of terrorism in realising its insidious goals is largely determined by the sense of terror which may be infused across all sections of society. Terrorism thrives on publicity and modern communication technology enables terrorists to penetrate collective consciousness and to vicariously expose the global community to the pain and suffering of the victims and their families. Besides, by propagating their convoluted ideological discourses with *pseudo-religious fervour*, the terrorist organizations partially succeed in bringing potential fence-sitters, sympathizers and ideologically aligned individuals into their folds. The dreaded and perfidious ISIS has transformed the way the terrorist groups reach and recruit followers globally and has become an *expansive enterprise* making *unsubstantiated and/or fraudulent* claims of religious or political legitimacy. By fanning religious fervour, nurturing hatred, perpetuating violence, committing acts of unprecedented cruelty and taking advantage of ignorance, the ISIS ensures that their ranks are filled with committed recruits.

The transformative power of new media and social networking platforms has been woven into the terrorist enterprise of ISIS almost from its inception. In the wake of ISIS offensive in June 2014, a number of Twitter accounts came up claiming to represent ISIS in Syria and Iraq. During the initial days of offensive, the various Twitter accounts were giving live updates and images of its advances in Syria and northern Iraq.

The ISIS digital footprint on social media kept pace with its advances made in Syria and Iraq. The images of captured Iraqi security personnel went viral garnering an even wider online audience. In an attempt to fan the religious jingoism, the information including number of bombings, suicide missions and assassinations it has carried out was shared on the growing number of Twitter accounts having large followings. In an attempt to expand its digital reach on social media, ISIS branched out to other platforms like YouTube, Facebook and Instagram. ISIS shocked and enraged the whole world when it posted the video of the beheading of American and British journalists and other innocent individuals. The deliberate attempt of ISIS to take its social media strategy to a whole new level is probably stemmed from its belief that the overly shocking and terrifying events posted online attract maximum viewership and may accomplish the objectives of their propaganda campaign.

The war against ISIS is fought by many nations- at times in a wary collaboration, at times in an open alliance- in many forms at various locations. The opening of another front against ISIS in virtual world, the cyber warriors – some *government affiliates, others driven by a sense of outrage* at *ISIS's* brutal reign of terror- in an effort to deprive the group of opportunity to use cyberspace for online propaganda, are trying to shut down ISIS supporters' media account and portray the group in its true evil and demonic form. The hackers and cyber experts on government payrolls –for the most part being in cat *and mouse relationship- have joined hands to fight a common enemy.*

One day after the attacks in Paris on November 13, a video was released on line supposedly by hacking group *Anonymous* proclaiming "we are uniting humanity, expect us." In the days that followed, the members of the group took out the Twitter accounts believed to be that of supporters and sympathizers of ISIS and some directly handled by ISIS operatives.[1] Behind the Guy Fawkes masks, '*Anonymous hacktivists'* have rallied under the banner '#OpParis' and have vowed to oust ISIS operatives from social media. Another group called 'Ghost Security' with the self-declared mission of targeting "Islamic extremist content" from "websites, blogs, videos, and social media accounts," claims to have carried out Distributed Denial of Service (DDOS) attacks against ISIS linked websites resulting in disruption or in taking down of more than 130 ISIS-linked websites by overwhelming their servers with fake traffic from multiple sources. [2] Another group called 'CtrlSec', closely related to 'Ghost Security', claims to have made elimination of pro-ISIS accounts on Twitter its sole mission.

The intentions of these *hacktivists* are gallant and brave, but the outcome of these operations may not meet the expectations that had initially been perceived. The critics are questioning the effectiveness of these operations as there is no immediate and substantial reduction *in the barbaric dispensation among the ranks and files of ISIS's cadre.* In a study by 'Brookings Center for Middle East Policy' titled 'The ISIS Twitter Census', it was brought out that from September 2013 through December 2014, by conservative estimate at least 46,000 Twitter accounts were used by ISIS supporters. This figure leapfrogs to 70,000 accounts with the maximum estimate. Much of ISIS's social media success can be attributed to a relatively small group of hyperactive users, numbering between 500 and 2,000 accounts, which tweet in concentrated bursts of high volume.[3] The twitter account of ISIS supporters far exceeds in numbers in comparison to 'Anonymous' claim to have helped unplug.

However, some computer security experts have opined that the online war against ISIS may prove effective as a countermeasure to interrupt or prevent the process of radicalization before the social frustrations and religious sentiments manifest in violence and unbridled cruelty. In addition, the online efforts of ISIS in the luring young recruits with radical sympathies in its ranks will also be undermined. Battling the ISIS in cyberspace is not limited to just online vigilantes. Various government intelligence officials and cyber security experts have also spurred up their efforts in countering and curtailing propaganda of extremist groups. The "Think Again Turn Away" campaign on Twitter, launched in English in December 2013 by the United States Department of State is an effort to enter the war of ideas and win over hearts and minds of radicalized individuals on social media. This was broadened with a Facebook account in August 2014.[4]

Despite these efforts, the ISIS is still using the power of social media as a key instrument of *coercion*, *enticement*, indoctrination, proselytisation and propaganda for waging its own version of modern jihad. Its operatives have switched to more sophisticated form of encryption to evade detection. The messaging apps like WhatsApp, Viber and Telegram are increasing being used by ISIS and other militant organizations. As these messaging apps use sophisticated and end-to-end encryption, the shared messages- despite of their dark and insidious contents- cannot be decrypted even by app's creators, owners and developers. Other ISIS members have switched to the Internet's dark Web— its shadowy alter ego populated by illegal sites which enables routing of a user's communication through an unfathomable maze of networks obliterating the possibility of tracing its source. Some ISIS operatives have even resorted to offensive cyber tactics. A group called Cyber Caliphate urged its followers to use Twitter to spread propaganda. ISIS extremists online posted the hacked personal details, including mobile phone numbers of the heads of the CIA, the FBI and National Security Agency (NSA). [5]

The war against ISIS shows no sign of abating in spite of massive air strikes and efforts of well equipped multinational armies. However, the meagre success of various groups in containing the ISIS online activities in cyberspace is viewed with subtle optimism and as a minuscule precursor to the overall objective of decimating the ISIS and rid the world of its brutal and oppressive ideology.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] Mirren Gidda, " Cracking The Caliphate :Can hackers and Western securityservices win the online war against ISIS?, *Newsweek*, December 04, 2015.

[2] Simon Cottee, "The Cyber Activists who want to shut down ISIS," The *Atlantic*, October 08, 2015, at http://www.theatlantic.com/international/archive/2015/10/anonymous-activists-isis-twitter/409312//, accessed on 03 Dec 15.

[3] J.M. Berger and Jonathon Morga, "The ISIS Twitter Census," *The Brookings Project on U.S. Relations with the Islamic World Analysis Paper*, No. 20, March 2015, p.2.

[4] Rita Katz, "The State Department's Twitter War With ISIS Is Embarrassing," *The Time,* September 16, 2015, at http://time.com/3387065/isis-twitter-war-state-department/, accessed on 03 Dec 15.

[5] Ian Gallagher"ISIS 'cyber caliphate' hacks 54,000 Twitter accounts and posts phone numbers of heads of the CIA and FBI in revenge for the drone attack that killed a British extremist," *The Mail,* November 8, 2015, http://www.dailymail.co.uk/news/article-3308734/ISIS-cyber-caliphate-takes-54-000-Twitter-accounts-Terrorists-hack-social-media-site-spread-vile-propaganda.html, accessed on 03 Dec 15.