ExpertView
Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
15/17

NEW APPROACHES TO COMBAT THE SCOURGE OF TERRORISM IN CYBER SPACE

Gp Capt Ashish Gupta
Senior Fellow, CAPS
01 November 2017

The scourge of terrorism continues unabated exacting a heavy toll in terms of human lives, sufferings, depletion of resources and imbalance in demographic structure. Terrorism, in various forms and manifestations, has been practiced throughout history and across a wide variety of political ideologies.[1] There is no single accepted definition of terrorism and a multitude of meanings could be inferred in different contextual settings by different people. Similarly, the fluctuating ideological profiles and organisational structures as well as changing means and methods of most of the terrorist organisations have led to the circumvention of efforts by many to categorise terrorism in one genre.

Terrorism thrives on publicity and cyberspace facilitates 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, sympathisers and ideologically aligned individuals into their folds.[2] Cyberspace is used by terrorists as a key medium not only for coercion, enticement, indoctrination, proselytization and propaganda but also for planning attacks after garnering information from cyberspace about potential target's location, security arrangements, and post attack impacts. Cyber terrorism is the convergence of terrorism and cyber space, perpetrated for the attainment of potential objectives such as provoking societal disharmony and radicalising people along sectarianism and religious fault lines.

In one of the report published by Europol, it was reiterated once again that Internet has become the principal means of communication for terrorist and violent extremist individuals and groups.[3] The online presence of such groups is frighteningly disturbing and horrifyingly substantial and provides these groups means and platform for the facilitation of activities contributing to or enabling terror.

The Internet is used for a range of purposes, including instruction, propaganda, recruitment, dispatch of members to conflict areas, fundraising, cooperation with other terrorist organisations, and the planning and coordination of attacks.[4] The use of cyber technology for committing, aiding, abetting, facilitating terrorism primary or secondary terrorist acts can be described as 'cyberterrorism'. Cyberterrorism has emerged as an attractive and cost effective option for terrorists offering significant benefits from a logistical, operational and consequential standpoint and a wider media appeal perspective.

Terrorists have relied on high profile violent acts, committed to bring in sharp focus their ideology, cause and narrative as well as to showcase their capabilities and intent as a terror outfit. In addition, contemporary terrorist groups leverage Internet for exerting psychological pressure over a global audience heightening fear psychosis and fanning communal polarisation. While analysing the dimensions and dynamics of international terrorism, Brain Jerkins articulated that, "Terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press. Terrorism is aimed at the people watching, not at the actual victims. Terrorism is a theatre."[5] The spectacle of carnage and violence is played out over and over again in the news and social media, watched by a global audience. For the terrorist, as Schmid and de Graaf have pointed out, the "immediate victim is merely instrumental, the skin of a drum beaten to achieve a calculated impact on a wider audience. As such, an act of terrorism is in reality an act of communication. For the terrorist the message matters not the victim".[6]

The publicity is a means of sustenance and survival of terrorism and Internet provides necessary scaffolding to publicise, plan and orchestrate terrorist activities and attacks. The emergence of "mass-mediated" terrorism is largely attributable to the exploitation of global networks and information highways by terrorists to propagate their mistaken and misplaced ideology as well as to expose the masses to the spectacle of violence as vividly as possible.

Islamic State (IS) Apocalypse: Bolstered by the Cyberspace

The digital technology is responsible in more than one way for setting in motion the juggernaut of terror and violence by the jihadist group Islamic State (IS). A number of political faux pas, misinterpretation of historical events, misreading of cultural sensibilities and a sense of collective victimisation: all these facilitated a 'limited Islamist insurgency' transforming into one of the most dreaded terrorist organization the "Islamic State (IS)". By using technology in many ingenious ways, IS was able to capitalise on alienation and existential concerns of a large population and became most brutal extremist Jihadi terrorist organisation the world has ever seen.

In an effort to stem the tide of cyber terrorism sweeping the region, the British Parliament is likely to enact a law that will make viewing of terrorist content online a criminal offence, with provisions for imprisonment up to 15 years. Ms. Amber Rudd, the British Home Secretary, announced that she wanted to make sure those who view despicable terrorist content online, including jihadi websites, far-right propaganda and bomb-making instructions, face the full force of the law.[7]

The proposed amendment to law will make it a punishable offence to be in possession of information likely to be useful for terrorists, or commission or attempted commission of a terrorist act. This will plug a loophole that allows people to watch videos meant for enticing, indoctrinating, persuading and coercing others to join or help terrorists with impunity and without any fear of consequences. Currently the law is applicable for online material that can be downloaded and stored on the computer, transferred and saved on a separate device or printed off as a hard copy. According to the BBC, "the new offence would apply only to those who repeatedly viewed online terrorist material, to safeguard those who click on a link by mistake or who could argue that they did so out of curiosity rather than with criminal intent".

To combat the scourge of terrorism, it is imperative to have strategic plans and their execution at the situation-specific tactical level. Such actions, coupled with intuitive ingenuity and intuitional perceptions may stem the spate of insurgency and terrorism in cyberspace.

(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])

Keywords: Terrorism, Islamic State, Cyber, British cyber laws

Notes

[1] Harvey Kushner, *Encyclopaedia of Terrorism,* (California, Sage Publications, 2003), p. xxiii.
[2] Ashish Gupta, *Cyber War: Conquest over Elusive enemy,*(New Delhi: KW Publishers, 2017), p. 241.
[3]Europol "EU Terrorism situation and Trend report", https://www.europol.europa.eu/newsroom/news/eu-terrorism-situation-and-trend-report-te-sat-2012, accessed July 20, 2017.
[4] Ibid.
[5] B Jenkins, "International Terrorism-A new mode of Conflict", https://www.ncjrs.gov/App/Publications/ abstract.aspx?ID=30518, accessed July 20, 2017.
[6]Brigitte Nacos, *Mass-Mediated Terrorism:The Central Role of the Media in Terrorism and Counterterrorism*, (Rowman & Littlefield: Plymouth, 2007), p. 14.
[7] UK News, "15 years in jail for watching terrorist videos," *The Week*, October 03, 2017,