Contemporary Terrorism and Technology

Prashant Kandpal

Islamic Theology of Counter Terrorism

اسلامک تھیولاجی آف کاؤنٹر ٹیررازم

Technology and Terrorism though being two totally different terms have established great connections in the past few decades, wherein former has been exploited by the later up to an optimum level. Technology, that can be defined as an application of scientific knowledge in routine life, has actually made a dramatic shift in *homo sapiens'* way of living. On the other side understanding the concept of/behind Terrorism has always been in debate. Inclusion of subjectivity has always been an impediment to understand this subject; the categorisation of terrorism as *good terrorism and bad terrorism*[1] and platitude like "one man's terrorist is another man's freedom fighter" has clearly proven the way subjective nature has been assigned to this term, even though the aim of generating fear has always been paramount for the terrorists. However, it can be defined as "a purposeful human activity directed toward the creation of a general climate of fear designed to influence in ways desired by the protagonists, other human beings, and through them some course of events."[2]

Our imagination of a terrorist has always been a bad guy holding an AK-47 and Rocket launcher wearing a bullet garland but with the advancement of technology, over the past few decades this image has changed. The *modus operandi* of terror outfits starting from the radicalization phase and till the execution of their plan has made a dramatic shift. Technology advancement has not only helped them in improving their approach but also given them an additional privilege of global reach. This report will look in different ways of how modern age terrorists have exploited technological advancement to achieve their aim. To dwell out the new *modus operandi* of terror outfits, case studies have been included in the paper. Results show how sophistication has been injected in this low-tech unconventional form of warfare.

The contemporary terrorism has set a new narrative in front of the whole world. The usage of technologies, internet in particular, has greatly impacted the growing terrorist threat and has amplified the reach of these outfits. But this is not something new, Ramzi Yousef who was convicted for 1993 World Trade Center bombing took advantage of computer technology in executing his plans, he was using a laptop with encrypted information. When the laptop was recovered by law authorities it took about a year to decrypt the files. Decryption of the laptop revealed his plan to destroy 11 US airliners in a coordinated operation. The second known attack on the World Trade Center of 9/11 was not only one of the deadliest and shocking attacks ever carried out by any terror outfit, but also showed the tactical innovation of terrorist organisations. These tactical innovations have been augmented by significant technological developments and motivational factors, most prominent of them are religious ideologies. The Mumbai attacks of 26/11 also shows how technological advancement has helped terrorists find new approaches in order to achieve their goals, this attack was considered as one of the most technologically advanced attacks ever executed. These terrorists came armed not only with AKs and grenades but also with GPS, cell phones, satellite phones and other high-tech military gears. For the first time an attack was coordinated remotely from a control room setup specifically for this attack and from where these terrorists were getting orders.

The terrorists navigated across the Arabian sea to Mumbai using a global positioning system, they used satellite phones to communicate with their handlers. In the three day siege the handlers sitting remotely

[1] Arinam De, "Did Pakistan Army chief just admit to sponsoring terrorism in India?", Daily O, February 20 , 2018 https://www.dailyo.in/politics/pakistan-admits-sponsoring-terror-munich-security-conference-general-bajwa-fatf/story/1/22464.html

[2] Actual Citation: H.H.A. Cooper

guided the terrorists about the ground situation using information coming on the NEWS channels and communicated with terrorists using internet phones that made the call tracing process complicated for the Indian authorities.[3] Such incidents show how technology is being exploited by the terror outfits.

One of the most dreadful terror outfits of the decade is ISIS (Islamic State of Iraq and Syria) that gained international media attention in the aftermath of Arab Spring. This organization made optimum use of the internet and has also proved that how technology can be molded otherwise. But if we compare ISIS with Al-Qaeda (Another terror outfit active in the Middle East and Africa) there are some discrepancies that we can see and these can be found in the answers of some questions. Why have ISIS regime's achievements been compared to that of Al-Qaeda's regime? Why was ISIS able to draw the attention of the whole world in a small period? How did it manage to become the richest terror group? Why did radicalized youth join this group in large numbers? The answer to all these questions is "Internet". Taking lessons from Arab-spring, ISIS also resorted to the heavy use of the internet especially for fundraising, operation planning, propagandas videos and recruitment.

The most prominent usage of the internet was done for the recruitment; ISIS began recruiting foreign fighters over the internet by producing very sophisticated videos that attracted many young recruits to join this terror outfit. ISIS used the internet to spread their propaganda videos that showed luxurious life under regime, camaraderie among terrorists, beheadings of what they call apostates and praising martyrdom to lure youths from different parts of the world. They urged people to support the caliphate by joining them or by carrying out attacks in their own country. In addition, they also made their presence in Facebook and Twitter. In the case of ISIS twitter always remained their favourite medium in order to sensitize the audience and attract *jihadis*. Not only ISIS, even Al-Qaeda and their affiliates have also resorted to social media especially twitter for recruitment purposes.

According to a report of New York Times during the first half of 2016, twitter suspended around 235,000 accounts that were somehow related to terrorism.[4] Facebook also wielded out advanced tools to remove extremists accounts related directly or indirectly to terror outfits. Twitter and Facebook both faced high pressure from various state's governments to take strict measures against extremist channels active on their platforms. After such strict measures by these two social media giants, terror outfits resorted to messaging services such as WhatsApp, Telegram, that have an end-to-end encryption of messages and are complex to be monitored by law enforcement agencies. Another way which terror outfits have adopted to spread their propagandas is by using blogs. One such blogging platform is Tumblr that has been extensively used by ISIS in spreading their propaganda, as it provides individuals to operate their columns anonymously.

The advent of internal messages and communication platforms in gaming consoles set another benchmark in the field of technology. Most of us must have played computer games like Call of Duty, Counter-Strike, PubG; these games are programmed with an internal communication platform wherein you can communicate with others either verbally or nonverbally and also allows you to download and

[3] Jeremy Khan, "Mumbai Terrorists Relied on New Technology for Attacks", The New York Times, December 8, 2008, https://www.nytimes.com/2008/12/09/world/asia/09mumbai.html

[4] Katie Benner, "Twitter Suspends 235,000 More Accounts Over Extremism", The New York Times, August 18, 2016, https://www.nytimes.com/2016/08/19/technology/twitter-suspends-accounts-extremism.html

save your files. These low tech systems can be misused easily; for instance, the case of a 14-year old boy from Austria who was convicted and sentenced two years jail term for downloading bomb making plans onto his PlayStation games console[5] .In addition the above incident, though not fully proofed still there are reports stating that ISIS employed PS4 (PlayStation 4) for 2014, Paris attacks.[6] Though it was not made clear till last whether PSN (PlayStation Networking) were used in plotting Paris attacks or not but the probability of misuse of such platforms is very high. Wikileaks documents have revealed that intelligence agencies were snooping in the virtual world and various gaming networks for the purpose of gathering information and making informers, probably because they must have considered it as a "target-rich communication network".[7] But is it really possible for terrorists to communicate on gaming networks? Can they be easily traced or not? If not, then what restricts intelligence agencies in putting a track on them? The communications in these gaming networks can be easily done between two or more individuals in both ways verbally through voice communications and messages or non-verbally an example for this could be writing messages on wall by spraying bullets that will vanish within seconds (though sounds dumb but an effective way).

These communications are encrypted with TLS (Transport Layer Security). TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions[8] and works on three main components- Encryption: hide the data so as to avoid it being transferred to third parties, Authentication: ensures that information is exchanged between actual/valid parties, and Integrity: deals with verification of forging or tampering of data. Decryption of data requires key and also in order to monitor these communications agencies need to breach the layer this can be done through breaching attacks that can exploit the vulnerabilities of TLS. But continuous upgradation of the security layer sometimes makes it hard for monitoring agencies to breach the layer and also makes the attacks more complex in nature, thereby making it hard to monitor these communications. The rising numbers of PlayStation, Xbox and other gaming network users all over the world also makes this process more critical and complex. PSNs if in case misused by terror outfits will be providing them a new medium to communicate, by maintaining their anonymity and targeting mass users with diverse thought processes.

The use of visual and print media as a medium to reach a mass audience has also surfaced in the recent decades. Observing the past trends of how terror outfits have indulged themselves and invested in their media campaign, one can say that the scientific fact that about half of the human brain is directly or indirectly devoted to processing or analyzing visual information has very well exploited these terror outfits mainly ISIS, AL-Qaeda. Since the beginning of ISIS regime, we have seen how they have used visual media to spread their Islamic ideologies, idea of Islamic caliphate, glorified beheadings and killings, and encouraged mass audiences to commit lone wolf attacks. During the peak of ISIS regime these videos had attracted many fanatics and many foreign fighters came and joined ISIS. Now when all

[5] Teenager in Austrian 'Playstation' terrorism case gets two years, Reuters, May 26, 2015, https://www.reuters.com/article/us-mideast-crisis-austria/teenager-in-austrian-playstation-terrorism-case-gets-two-years-idUSKBN0OB0LK20150526
[6] Paul Tassi, "How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks", Forbes, November 14, 2015,https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/#1c8dc4c77055
[7] Justin Elliott, "World of Spycraft: NSA and CIA Spied in Online Games", ProPublica, December 09, 2013, https://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games
[8] Zeus Kerravala, "What is Transport Layer Security (TLS)?",Network World, November 09, 2018, https://www.networkworld.com/article/2303073/lan-wan-what-is-transport-layer-security-protocol.html

are thinking that ISIS is gone, ISIS sponsored media platforms are working hard on their propaganda videos for their resurgence. They are not only active in visual media but also very much active when it comes to print media like magazines and various posters. Their magazines generally include interviews of commanders, articles praising the dead terrorists as a martyr, urging others to commit *jihad*. The foundation of ISIS media production was laid in 2006 with the formation of *Al-Furqan* media production institute, main functions of this institute was to glorify the image of the caliphate by producing films, posters and statements from commanders. Further IS established *Al-Hayat* in 2014 whose main function was to publish caliphates video and also magazines, there have been reports of a radio channel *Al-Bayan* also.[9] Unlike ISIS, Al-Qaeda has been more focused towards their mission and terror control through traditional ways.

One can also say that when compared with opportunistic ISIS, Al-Qaeda is less tech savvy and therefore not managed to get that support that ISIS managed with a span of two or three years. But Al-Qaeda in Arabian Peninsula (AQAP) an affiliate of Al-Qaeda active in Yemen and Saudi Arabia has managed to run their propaganda production house. They published "*Inspire*" magazine in 2010 this magazine's main purpose was to reach its supporters and sympathizers, and make them aware of their missions, urging them to do jihad, one such edition also published an article of how to make bombs at home. In 2018, AQAP inaugurated *Al-Badr* media foundation with the aim to publish videos, documentaries and magazines to maximize their reach and to incite Muslims to join their organization.[10] This traditional media game played by terrorist organizations is creating a sense of "real competition" between them in order to prove them victorious in this propaganda race and to achieve hegemony over others.

With increasing technological advancement there is a need to keep a continuous eye on threat and a professionalism while assessing threat. In this era of technology, terror outfits active across the world are extensively exploiting the vulnerabilities present in the inventions be it an open cyberspace or a race for nuclear warheads. Our negligence towards the vulnerabilities of new sophisticated technologies will act only as an impediment to assess the cause, dynamics and outcomes of their misuse by terror outfits. The traditional terrorism that was limited to a particular territory with political, religious and ideological propaganda has now taken the shape of "non-territorial terrorism", aiming not only the seizure a particular territory but towards a bigger goal of global destabilization. Our proactiveness towards vulnerabilities of new technology and measures to neutralize them can defeat the aim of terror outfits.

***ITCT** does not necessarily endorse any or all views expressed by the author in the article.*

[9] Katie Cohen and Lisa Kaati, "Digital Jihad- Propaganda from the Islamic state", November 2018,

[10] Al-Qaeda in the Arabian Peninsula,Counter Extremism Project, https://www.counterextremism.com/threat/aqap-al-qaeda-arabian-peninsula