TECHNOLOGY SOLUTIONS TO REINFORCING SECURITY

By Maj Gen P K Mallick, VSM(Retd)

Introduction

21st century is characterized by phenomenal growth of technology specially Information Technology (IT) and Internet. The technology is becoming cheaper, easy to operate and provide facilities which could not be even imagined decade earlier. Technology is also a great leveler. Today the same facilities provided by latest technology advancements are available to violent elements as well as law enforcing agencies and armed forces. Today's enemies are dynamic, unpredictable, diverse, fluid, networked and constantly evolving leading to complex problem sets. Small networked organizations like insurgents are very good at adopting technology whereas large, hierarchical, bureaucratic Government organizations take its own time to exploit its benefits.[1] Technology is central to both terrorism and counterterrorism, yet each side sees technology in a different way.

Social media has helped like minded people around the world to connect. It has also aided the causes of violent extremists by networking them to similarly inclined individuals and organisations. Terrorists excel at exploiting opportunities, But terrorists did not create Twitter, YouTube, or Facebook – although they have used these platforms extensively. The introduction of artificial intelligence, machine learning and natural language processing technology to identify and remove terrorist content online is a positive move to make the Internet safer. Responsible leadership and decision making are required from governments and technology firms to deliver the products and services needed to reap the benefits of innovation and make technology work for everyone.

Use of Technology by Law Enforcing Agencies

There are a number of challenges that policymakers face today in the ever increasing reliance on technology for countering terrorism today. These include:

- The level of engagement with the communities affected by the technology implementation.
- The effectiveness of counterterrorism measures.
- The resources dedicated to counterterrorism.
- Achieving an appropriate balance between privacy and security.
- Data sharing challenges.
- Respect for criteria of legitimacy, necessity and proportionality.

---

[1] Brig P K Mallick, Leveraging Technology in CI Ops, Pinnacle, Jun 2008 available at : https://drive.google.com/file/d/0B7lCgXHBh1PaTlQ3VVZYbFRWbXM/edit

Technology can help to :

- Understand the causes of radicalization.
- Protect the national infrastructure.
- Reduce the vulnerability of crowded places.
- Protect against cyber terrorism.
- Improve analytical tools.
- Identify, detect and counter novel and improvised explosives.
- Understand and counter chemical, biological, radiological, nuclear and explosive threats (CBRNE).

Communications. Counter terrorism efforts force terrorist groups to change how they communicate. The U.S. government used its military and intelligence assets against al Qaeda following the 9/11 attacks and the invasion of Afghanistan. Many al Qaeda leaders hiding in Pakistan were tracked down and captured because of sloppy communication methods. Identifying and tracking al Qaeda communications networks was so successful that it forced Osama bin Laden to shun electronic communications devices altogether, relying instead on human couriers as a link to the outside world. But the terrorists also adapted.

Use of Internet

The Internet could be exploited by terrorist organizations for several purposes including:

- Propaganda.
- Psychological warfare.
- Recruitment and mobilization.
- Fundraising.
- Data Mining, information gathering.
- Secure communications.
- Cyber attacks.
- Software distribution (e.g., mobile app).
- Buying false documents.
- Training.

Bitcoins

Bitcoins and similar crypto currencies have become attractive to terrorists who see them as a means to solicit donations, purchase or sell weapons in the dark web and move funds globally to boost their financial capacities. Crypto currencies are privacy-focused and thrive on a decentralised financial ecosystem. This allows cyber criminals to circumvent financial institutions and their operational tools which have been designed to counter terror funding. The high profit rate and value volatility of

crypto currencies may lead to its large scale adoption by extremist groups which are desperate for new fundraising mechanism to sustain their activities.[2]

Dark Web

The layers of the Internet go far beyond the surface content that many can easily access in their daily searches. The other content is that of the Deep Web, content that has not been indexed by traditional search engines such as Google. The furthest corners of the Deep Web, segments known as the Dark Web, contain content that has been intentionally concealed. The Dark Web may be used for legitimate purposes as well as to conceal criminal or otherwise malicious activities. It is the exploitation of the Dark Web for illegal practices that has garnered the interest of officials and policymakers.

Anonymizing services such as Tor have been used for legal and illegal activities ranging from maintaining privacy to selling illegal goods—mainly purchased with Bitcoin or other digital currencies. They may be used to circumvent censorship, access blocked content or maintain the privacy of sensitive communications or business plans. However, a range of malicious actors, from criminals to terrorists to state sponsored spies, can also leverage cyberspace and the Dark Web can serve as a forum for conversation, coordination and action.

Just as criminals can rely upon the anonymity of the Dark Web, so too can the law enforcement, military and intelligence communities. They may use it to conduct online surveillance and sting operations and to maintain anonymous tip lines.

Anonymity in the Dark. Web can be used to shield officials from identification and hacking by adversaries. It can also be used to conduct a clandestine or covert computer network operation such as taking down a website or a denial of service attack or to intercept communications. Reportedly, officials are continuously working on expanding techniques to deanonymize activity on the Dark Web and identify malicious actors online.[3]

Terrorists are using "virtual safe havens" using encrypted communication channels, hidden portions of the internet, cryptocurrency accounts that are not registered with any banks and more. Pseudo-anonymity offered by darknet makes the dark web an ideal environment for various activities such as:

- Propaganda
- Purchasing weapons

[2] Ahmad Helmi Bin Mohamad Hasbi and Remy Mahzam, Cryptocurrencies: Potential for Terror Financing? S. Rajaratnam School of International Studies (RSIS), 30 April 2018 available at : https://www.rsis.edu.sg/wp-content/uploads/2018/04/CO18075.pdf

[3] Kristin Finklea, Dark Web, Congressional Research Service, March 10, 2017 available at : https://fas.org/sgp/crs/misc/R44101.pdf

- Purchasing stolen card data
- Counterfeit documents
- Recruiting
- Download Mobile Apps used for secure communications
- Purchase of malicious code
- Encryption to hide
- Cryptocurency to evade detection and to fundraise.

The following is recommended [4] :

- Technology companies should create a self regulatory system to remove and audit extremist content and release publicly available annual reports outlining their efforts in this space.

- The Government should create an internet regulation body.

- More resources should be dedicated to the joint terrorism analysis centre (JTAC) to build intelligence capital on the darknet.

- Social media companies should work with law enforcement agencies to ensure that extremist material is not simply removed but archived effectively to understand patterns of behavior.

Social Media

Terrorists use the new social platforms like Facebook, Twitter and media services such as YouTube for propaganda. Some of the groups have a great mastery of the technology and a deep knowledge of the techniques of communication. Each video is carefully prepared. The programming is meticulous and aims to reach the largest number of individuals. Their language is direct, young, and it can reach a specific audience by using images with a high emotional impact. The amplification effect is obtained through easy dissemination of content, sympathizers and media outlets allow easy sharing of the terrorist messages through emails, messaging and mobile apps like WhatsApp. In J&K the terrorists have shown their ability to whip up emotions through social media.

Social media is not the cause of violent extremism, but a powerful amplifier and accelerant. Digital platforms and increased access to smart phones and internet connectivity help facilitate radicalization and recruitment. The terrorists' exploitation of digital platforms allows would be terrorists to seek inspiration and information online and rally around a terrorist group as a brand, an idea or a methodology

[4] Nikita Malik, Terror in the Dark: How Terrorists use Encryption, the Darknet, and Cryptocurrencies, The Henry Jackson Society, 2018 available at : http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

without ever leaving their homes. The widespread use of social media has also made violent extremists' plans more difficult to disrupt. Security agencies have to track a much larger number of potential plotters, giving terrorists more space to plan large, complex operations against a higher background level of activity.

A special report by the US Department of Homeland Security listed various terrorist uses of Facebook:[5]

- As a way to share operational and tactical information, such as bomb recipes, weapon maintenance and use, tactical shooting, etc.

- As a gateway to extremist sites and other online radical content by linking on Facebook group pages and in discussion forums.

- As a media outlet for terrorist propaganda and extremist ideological messaging.

- As a wealth of information for remote reconnaissance for targeting purposes

The technology firms have faced increasing pressure from governments across the globe to stop the spread of extremist propaganda. Last year, White House officials met with Apple, Facebook, Twitter and Microsoft to discuss the subject. The British prime minister, Theresa May, has recently renewed her campaign against the technology companies with a crackdown meant to punish platforms that fail to take sufficient action against terrorist propaganda. At a recent bilateral meeting in Paris, May and French president Emmanuel Macron said they would explore new legal liabilities for tech companies that don't remove inflammatory content, including possible fines.

While governments have urged companies like Facebook to do more, the social network has also faced backlash for ethically questionable censorship of non-terrorist content under the guise of countering propaganda.[6]

Use of Social Media by Law Enforcing Agencies

However, Social media analysis has significant potential to support counter terrorism operations by providing a window into the perspectives, thoughts and communications of a wide range of relevant audiences. These platforms can provide important information on a group's or audience's demographics, size, organizational

[5] Weimann, Gabriel. New Terriorism and New Media. Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014 available at http://www.wilsoncenter.org/publication/newterrorism-and-new-media

[6] Sam Levin, Tech giants team up to fight extremism following cries that they allow terrorism, The Guardian, 26 June 2017 available at : https://www.theguardian.com/technology/2017/jun/26/google-facebook-counter-terrorism-online-extremism

structure, areas of activity and network reach. Such details can inform efforts to target messages to particular audiences or influence perceptions, decisions, or behavior. Social media analysis can identify individuals who are becoming radicalized, measure the prevalence of support for extremist causes among particular demographics and gauge the depth of this support.[7]

Role of Technical Firms

The tech firms have long struggled to balance their missions of supporting free speech with the need to remove and prevent the spread of terrorist content. The companies have faced intense scrutiny over the way terrorist groups have used the site for recruitment and for spreading hateful and violent messages. On Jun 25, 2017 Facebook, Microsoft, YouTube and Twitter collectively announced a new partnership aimed at reducing the accessibility of internet services to terrorists. The new Global Internet Forum to Counter Terrorism adds structure to existing efforts by the companies to target and remove from major web platforms recruiting materials for terror groups. Together, the four tech leaders say they will collaborate on engineering solutions to the problem, sharing content classification techniques and effective reporting methods for users. Each company also will contribute to both technical and policy research and share best practices for counterspeech initiatives.

Privacy vs Security

With the introduction of end to end secrecy government intelligence agencies are unable to monitor the terrorists communication**.** Law enforcement and security agencies have claimed that encrypted platforms built for commercial purposes to safeguard privacy—where only the sender and receiver hold the keys and devices to decipher the message—are a gift to terrorists and criminals to help them communicate in a way that puts them beyond the law's reach.

Tech companies have resisted any push to hand over to law enforcement agencies the keys to their customers' encrypted data. Privacy advocates have, defended the technologies as a protection against government snooping. But tech companies, are arguing that there are real risks of going along with government requests to access encrypted messages. Apple CEO Tim Cook, for example, recently warned that 'any back door is a back door for everyone. Everybody wants to crack down on terrorists. Everybody wants to be secure. The question is how. Opening a back door can have very dire consequences.'

[7] William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, Monitoring Social Media Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations, Rand Corporation, 2017 available at : https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1742/RAND_RR1742.pdf

When it comes to privacy and security, we need to find the right balance in not allowing new encryption technologies to obstruct our counterterrorism efforts. We need secure encrypted systems for commerce, government and the protection of personal information (our digital identity). Banks and telcos are using those products to safeguard our data. Deliberately weakening encryption solutions would arguably weaken key infrastructure, with the ultimate beneficiaries being criminals, cyber activists and rival nation states. A cooperative solution with our police and security agencies working with relevant companies to identify the problems would be better than trying to introduce laws to restrict encryption. [8]

Latest Technologies in Counter Terrorism Operations[9]

Big Data

In order to fight the terrorists, it is critical to get an in depth understanding of that enemy, how they operate, what technology they use. Big data gives a better insights into their activities. The data can be used to get an understanding of backgrounds, motives, modus operandi, methods of communication. Once these elements are understood, the information can be leveraged to learn about terrorist networks; who finances them, who supplies them, who supports them and who are the informants. Big data can also be used to establish patterns and make predictions on which population groups or what type of person would be most likely to join a terrorist organisation.

Drones

Surveillance data from drones gathered in areas where suspicious activity is taking place can also provide valuable information, especially when this real time information is combined with other data sources. Information like this can help establish connections between people and events and identify the location of terrorists and even make predictions of the where they may move to in the future.

Robots

At the World Robot Conference in Beijing, China recently unveiled toy-sized battle robots with grenades and assault rifles. These robots have been designed in three versions: an attacker robot – armed with grenade launchers and rifles that minimise recoil – a reconnaissance robot capable of detecting hazardous gases and a bomb disposal robot. Another robot used in the war against terrorism is the PackBot – a

[8] Anthony Bergin, Encryption technologies and counterterrorism, The Strategist , The Australian Strategic Policy Institute Blog, 30 Nov 2015 available at : https://www.aspistrategist.org.au/encryption-technologies-and-counterterrorism/

[9] Can we combat terrorism with technology? March 24, 2016 available at : https://www.richardvanhooijdonk.com/en/can-combat-terrorism-technology/

machine that locates and diffuses bombs. The PackBot will eventually carry out complex tasks without any human interference and will be very effective in detecting terrorists and explosives. PackBot can gather information from devices such as streetlights, bus shelters and sensors and combine it with its own data to make decisions. Various countries are developing autonomous robots that are able to eliminate terrorists and free hostages. These bots will be outfitted with biometric recognition technology and connect with sources that supply image data and location information to help identify potential terrorists.

Predicting the Unpredictable.

The use of prediction software in the fight against terrorism is also referred to as ‘predictive policing’. This form of counterterrorism has been on the increase and the ISS (Intelligent Software Solutions) behavioural analysis tool Dfuze is already used in over forty countries. Dfuze was used at the 2012 Olympics in London to pinpoint high risk areas to enable police forces to increase security presence. The software was also used to investigate the Boston bombings in 2013. The Dfuze system is a database which holds information on all terrorist attacks that have ever taken place. Governments can access this data to analyse previous attacks and share information, leading to more efficient methods of communication between nations. With the Dfuze system, specialists are able to establish and analyse trends and patterns, future attack hotspots, the types of explosives, modus operandi and help them predict, prepare for or even prevent any future terrorist attacks. In the past, this type of work was done by analysts trawling through mountains of information, initially in paper files and later on computers.

Another predictive solution, launched in 2014, is Predictify Me. The technology is simple to deploy, can help predict an impending terrorist attack and secure areas against it. Predictify Me uses 200 indicators, such as public holidays, the weather, attacks in nearby countries, sports or other events and even video releases on social media to predict whether and when a terrorist attack is likely to happen. Predictify Me have indicated that it is able to predict an attack within three days with an accuracy of over 70 percent.

Internet of Things

With more and more devices connecting to not only the Internet but also to each other, the Internet of Things enables increased convenience, efficiency and energy conservation. With internet connectivity moving away from the traditional laptops, tablets and smartphones and migrating toward wearables and household devices such as fridges and washing machines, the IoT can also easily be used for monitoring, location tracking, identification, surveillance and gaining access to networks. Every device will have an IP address and security experts have indicated that surveillance services will able to intercept signals of networked devices in much

the same way as they intercept cell phone signals. Information from speeches, satellites, videos and news is all collected and used to monitor and analyse activities, enabling intelligence services to close in on terrorists.

Colour Changing Sensors

New colour-changing sensors can detect multiple explosives within seconds. In December 2015, scientists developed a new colour-changing sensor that is able to identify and quantify multiple explosives such as DNT, PETN, tetryl, RDX and TNT within ten seconds. The fluorescent sensor gives out information about the type of explosive and how much of it is present in a sample. PETN and RDX for example, have been used in terror plots because they are hard to detect by sniffer dogs. The colour changing sensor is made from light emitting nanomaterials or ‘quantum dots’ to which receptors that target the explosive are attached. Each explosive that binds to the quantum dot emits a different colour. These are then analysed in order to generate a unique ‘fingerprint’ for each compound. This makes it possible to detect multiple explosives with one single test.

Way of the Future

The United States and Israel reportedly caused actual damage to the Iranian nuclear program through malware such as Stuxnet. Russia has conducted cyberattacks against physical targets such as the Ukrainian power grid. With Stuxnet being reverse engineered by hackers, and other National Security Agency hacker tools made available through groups like Wikileaks, it is possible by the terrorists hackers to cause real world damage by simply accessing the internet.

Drones can be used for pre operational surveillance, propaganda purposes and attacks. The Islamic State have used altered conventional munitions such as 40mm grenades or military grade explosives placed in locally manufactured munitions. Hezbollah likewise has used drones in attacks. As technology advances, terrorists and counterterrorism forces will continue to use it to their advantage. It depends on who picks it up from the table first.

Challenges Ahead

Research and Development Trends. Most of the cutting edge research in related areas, particularly with regard to information technology and biotechnology, is in the private sector where development programs are largely driven by potential markets. The profits to be made in the security sector pale in comparison with other commercial opportunities. This challenge can be addressed by making the counterterrorism community a more attractive customer for the private sector.

Barriers to Innovation. Even if private research and development can be better teamed with government efforts and focused on the terrorism challenges of the 21st century, the traditional barriers to innovation in law enforcement technologies will remain. These challenges include four areas.[10]

- **Cost.** The expense of new technologies includes both the cost of procuring a technology and the opportunity cost of adopting that technology as compared to other uses to which resources might be put.

- **Technology Risk.** This includes the ever present risk that "big bets" will fail. The technology may not perform as expected or adequately address the tasks for which it was adopted.

- **Human Factors.** New counterterrorism technologies can face a plethora of obstacles that have nothing to do with fiscal costs or technical specifications. For example, data mining and biometrics have raised an array of concerns about the protection of civil liberties and safeguarding of proprietary commercial information. Non lethal weapons face legal barriers.

- **Unanticipated Costs.** Any new technology will bring unintended consequences. The introduction of nanotechnologies, for example, has raised concerns about the potential consequences of unintentionally introducing new compounds into the environment. New technologies can also bring unexpected liabilities and adverse public reactions.

Policy Recommendations

Counter-terrorism technologies and diverse partnerships are essential when dealing with terrorist threats in cities. RAND Europe's five counter-terrorism policy recommendations as given below are apt : [11]

- Deploy appropriate counter terrorism technologies that enhance decision making, but pay attention to the evolving technology landscape.

- Establish partnerships with all levels of national government, law enforcement agencies, private sector security companies and local authorities, while also collaborating with international partners and allies.

[10] James Jay Carafano, Ph.D, The Future of Anti-Terrorism Technologies, The Heritage Foundation, 6 June 2005 available at : http://www.heritage.org/homeland-security/report/the-future-anti-terrorism-technologies

[11] Susanne Sondergaard et al, Tactical Approach to Counter Terrorists in Cities, Rand Europe available at : https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1287/RAND_RR1287.pdf

- Where possible, engage with the public, the media and local communities when deploying new counter terrorism technologies, such as surveillance systems.

- Carefully consider the extent to which data collection and data sharing during a counter terrorism operation are proportionate, necessary and justified.

- Identify and address any potential privacy issues as early as possible before introducing new counter-terrorism technologies.

Conclusion

The terrorists are proving more and more adept at using sophisticated technology. The terrorist threat against the free world is serious and enduring. We need to stay one step ahead and keep developing new, improved technology. We need to jointly develop the means and the technologies needed to meet this threat. The obstacles to creating an arsenal of counter terrorism technologies that are practical and affordable and overmatch the threat of 21st century terrorism are daunting. Creating a vision of these future technologies, implementing initiatives that broaden the market and make it more predictable and dependable and developing policies that will help to overcome the barriers to innovation are essential steps to harnessing technology to the future needs of law enforcement.

Maj Gen PK Mallick, VSM(Retd) has been a Senior Directing Staff(SDS) at National Defence College, New Delhi. He is an expert in Cyber Warfare, SIGINT and Electronic Warfare.