"Big Data" and Counter Terrorism-A Way Forward

Maryam Baloch

Abstract

The contemporary era of technological advancements provides a plethora of opportunities for counterterrorism efforts using Big Data. Big data constitute records of all digital information of both the past and the present from the beginning of the digital age. The generation of excessive data makes it difficult for authorities to analyze and is highly disorganized as well, so it becomes difficult to extract information quickly upon need. Applying qualitative method, this study explores how states can utilize information from the big data to form solutions to counter-terrorism efforts swiftly. From pointing out digital alternatives like the use of algorithms, employing tracking capabilities and integrating pattern recognition in surveillance systems etc. for terrorists, this research leads to provide some gainful plans to combat violent extremism through big data and discovering opportunities for Pakistan. It identifies current and future technical and operational difficulties and supports the use of Big Data for national security spheres.

Keywords: Counterterrorism, Big Data, Algorithms, Surveillance

Introduction

In the present era, data is being generated at a rapid speed from a wide range of sources. Now data companies have to deal with terabytes, petabytes, exabytes, zettabytes and even yottabytes. This complex, dynamic and massive volume of data is termed "big data" which can be in the form of structured, unstructured, or semi-structured, generated by different

platforms like the web, social media, finance departments, CCTV, mobile communication, radiofrequency, sensors, satellites and many more. In order to counter the spread of hate speech, threat of terrorism and violent attacks, this study has been analyzed to identify the significant suggestions from big data.

Terrorism has been a long-running challenge for the international community and is a hurdle for the growth of many developing countries like Iran, Pakistan, Afghanistan, Iraq, Syria and many more. Contemporary terrorist organizations are using computational methods concerning technological advancement. The study tends to find potential pathways to combat violent extremism via big data. These innovations are being produced to create ease in our life but are often used negatively by extremists or criminals. While numerous advantages of the internet are obvious, it might likewise be utilized to work with the transmission of information within the terrorist organizations and just as material help for arranged actions of illegal intimidation, all of which require explicit specialized technical information for the successful examination of these crimes.

In addition to all other opportunities in society, the technological advancements have brought ground breaking ideas for criminals, terrorists and other anti-social elements too, that are influencing societies in different spheres. The modern era demands inventive plans to combat extremist ideologies and violence. As all the web-based social media networks are relatively new, so ideas to combat criminal activities through this medium are still under research. Platforms including Facebook, Instagram and

Twitter have changed the way of interaction and thus provided new opportunities for extremists to propagate and create threats among people.

Additionally, criminals have also been using these social channels to communicate with each other regarding any criminal or terrorist act. Extremists are using these computational advancements for communication to spread hate and terror, get donors, propagate agenda, publicize crime, get sympathy and followers and even for training of their team members.[1] Being cheap, faster and easily accessible, these social media platforms can be considered facilitating factors for terrorists. Terrorist organizations, ISIS, Al Qaeda, Al Shabab, Boko haram and Revolutionary Armed Forces of Colombia (FARC) working namly through this medium are seen using hi-tech technologies and high-velocity content.[2] Not only social media, but a report also shows that terrorist organizations may use PlayStation games for communication because it is hard to decrypt information travelled through PlayStation games.

Mass surveillance programs have been conducted by different countries to collect relevant data to track down terrorist-related activities but stakeholders of those countries have also seen criticism for exploiting individual privacy over the digital domain. As there is no specific company or country that owns the data, states are getting conscious of their data being used by other states as a tool to contain them. This key issue of exploitation led the USA to ban eight Chinese applications including WeChat, TikTok

[1]Carol K. Winkler and Cori E. Dauber, *Visual Propaganda and Extremism in the Online Environment* (Carlisle, Pa: Strategic Studies Institute and U.S. Army War College Press, 2014).
[2]Martin Rudner, "'Electronic Jihad': The Internet as al Qaeda's Catalyst for Global Terror," *Studies in Conflict & Terrorism* 40, no. 1 (March 30, 2016): 10–23, https://doi.org/10.1080/1057610x.2016.1157403.

and Ali pay under the Trump administration. China and Russia are also under debate about manipulating the masses, as they are moving towards digital rule over the public and monitoring individual activities to track offenders through cyberspace.[3]

Qualitative analysis with a simple literature review has been made to look forward to potential ways to combat violent extremism through big data. Based on the literature evaluated for this research, there are numerous provisos in counterterrorism techniques in the contemporary era of Artificial Intelligence. The previously recommended strategies to battle extremism through big data examination are still lacking and are somehow not much adequate to deal with the current techniques of terrorists.

Primarily, this paper proposes the utilization of potential pathways to combat terrorism with the help of big data. Better solutions demand the utilization of appropriate Algorithms that separate relevant information from a variety of datasets along with utilizing decryption tools to analyze the encrypted data from hidden servers like the dark web. Relative opportunities for Pakistan are also presented, as Pakistan is right now lacking in the spheres of artificial intelligence.

Pakistan and Big Data

Pakistan is one of the states that have been affected most by terrorism. Pakistan has suffered huge human and financial losses. In the past decade, Pakistan did exceedingly well in countering terrorism especially in the Northwestern part but that success has only been through the use of military

[3]Peter Bergen et al., "Do NSA's Bulk Surveillance Programs Stop Terrorists?," *New America Foundation*, 2014.

operations.[4] The problem with most developing countries in general and Pakistan, in particular, is to pre-empt and respond to a terror attack before happening. With the herald of the cyber era, it is now in the realm of possibility for Pakistan to move towards advancements that would allow it to not only detect any incoming terror attacks but to put a stop to them pre-emptively as well. For this purpose, Pakistan needs to rely on Big Data. Due to restrictions imposed and the unavailability of necessary technology, many developing states have not been able to tap into the potential of Big Data in identifying or tracking suspected terrorists.

Since 9/11, Pakistan has been engaged in a ravaging war against terrorism within and beyond its boundaries. This war has resulted in countless armed encounters between terrorist forces and Pakistan forces leading to terrible consequences. The consequential losses Pakistan suffered during the two decades of war fighting against the terrorist forces resulted in a period of economic crisis for Pakistan from which return seemed like a dream.[5] This in turn led to a drastic decrease in development efforts of the country's infrastructure in the way of new forms of warfare that emerged along the way. The alliance of Pakistan with the US, which is a much more technologically advanced state, gave Pakistan a fighting chance with its superior technology like drones, ballistic missiles, defence systems and surveillance systems, etc.[6] Pakistan, while fully aware of the vulnerabilities

[4] Sardar Muhammad, "War as an Instrument of Political Policy: Clausewitzian Analysis of Operation Zarb-E-Azb," *Pakistan Social Sciences Review* 5, no. I (March 15, 2021): 314–28, https://doi.org/10.35484/pssr.2021(5-i)25.
[5] Muhammad Shahbaz, "Linkages between Inflation, Economic Growth and Terrorism in Pakistan," *Economic Modelling* 32 (May 2013): 496–506, https://doi.org/10.1016/j.econmod.2013.02.014.
[6] Fazal Wahid, "The US War on Terror in Afghanistan and Its Impact on FATA in Pakistan," *Global Social Sciences Review* IV, no. III (September 30, 2019): 17–24, https://doi.org/10.31703/gssr.2019(iv-iii).03.

that would arise in neglecting the cyber domain, was left with no other choice due to limitations that arose via the losses suffered in the war.

Now, Pakistan is on the track to getting back on its feet with the help of its sworn ally, China. Currently, it has started to work on the digital domains of warfare by launching various programs within the state to develop a credible workforce that can effectively tackle cyber issues and establish the basis for e-commerce purposes. There are a lot of areas in the cyber domain where Pakistan is lagging far behind. Big data is one of the resources of the digital domain that can help Pakistan in rivalling even the most advanced nations in the world. The utility of Big Data is almost non-existent in general let alone its specific use for countering terrorism.[7] Though there are many areas of counter-terrorism efforts that can be exploited using the big data streams, Pakistan is still lacking and is almost 5-10 years behind worldwide.[8]

Pakistan is on the gray list of the Financial Action Task Force (FATF). Using advanced methods for tracking money using big data analytics would help Pakistan to get its name removed from the gray list.[9] It is possible by using the techniques to track money laundering on digital platforms. Once Pakistan establishes big data servers within its borders, it can use algorithms instilled with various data sets of previous cases that were detected in

[7] Ahmed Mukhtar, "Use of Big Data – a Missed Opportunity," The Express Tribune, October 11, 2020, https://tribune.com.pk/story/2267971/use-of-big-data-a-missed-opportunity.

[8] zahid, Zeng, Zulfiqar, Sherish, Liu, *"A Review of Policies concerning development of Big Data Industry in Pakistan"* iCoMET 2018. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8346315

[9] FATF, "Follow-up Report to Pakistan's Assessment of Anti-Money Laundering and Counter-Terrorist Financing Measures," www.fatf-gafi.org, May 2021, https://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-pakistan-2021.html.

Pakistan to establish parameters for new patterns and unofficial transactions. The world is moving at a rapid pace with the developments in digital frameworks. Pakistan must keep up with it otherwise it will be left behind. To do so, it will have to adopt technological advancements.

The world is moving towards big data for handling almost all their affairs whereas, in Pakistan, no recognition has been given to the value of big data.[10] The negligible amount of work being done in Pakistan on the topic at hand is being carried out by private companies. Various firms like big players in the digital economy like Amazon, Facebook, Alibaba, etc. are becoming operational in Pakistan utilizing big data analytics to further enhance businesses, marketing and IT industries. The concerned departments seem to neglect the value that could have been generated by the use of Big Data. For a country like Pakistan, utilizing such measures could be very handy.

Given its history of terrorism, it is necessary to keep tabs on the people who have been previously involved in any such activities. Keeping a check on their texts, posts, calls, etc. and getting warned of any potential threat could cut down the number of activities by a big number. Pakistan has already done well in terms of military success. Now, the need is to sustain this environment of relative peace. For that, Pakistan would have to move towards technologically efficient Big Data sooner rather than later.

[10] Peter Layton, "Belt and Road Means Big Data and Facial Recognition, Too," www.lowyinstitute.org, June 19, 2020, https://www.lowyinstitute.org/the-interpreter/belt-and-road-means-big-data-facial-recognition-too.

Another problem facing Pakistan is the financing of terrorists. It is the reason Pakistan has been on the FATF's gray list for a while now.[11]The use of big data can also help Pakistan in this regard. The programs like "know your client" could immensely benefit Pakistan is not only getting out of the gray list but can also help the country trace the origin of any money that could be used in any future terrorist activities in its territory.[12]

Algorithms

To deal with big data, all types of methods required specific Algorithms. Algorithms are the programs that help to give shape to the chaotic streams of information in the big data servers. It is possible to use algorithms to run prediction programs on the big data servers to discover any planned activity of terrorists. Stannat and Mecacci in their paper "Machine learning against terrorism" investigate the mass surveillance program explicitly by the USA, UK, Germany, Sweden, France and the Netherlands. They suggest that algorithms should contain both the "positive or negatives" to maintain balance until a person is confirmed to be a terrorist or non-terrorist.

A spurious correlation is led by the over fitting in algorithms, as applying more datasets results in giving correlations that may be useless for intelligence officials. These challenges can give us false classification of threats too. Authors identify the difference between the algorithms used for local policing and counter-terrorism, as terrorist attacks are often led by

[11] Dawn.com, "SBP Prohibits Financial Sector from Dealing in Cryptocurrencies, Says It Will Take Action on Violations," DAWN.COM, April 7, 2018, https://www.dawn.com/news/1399997.

[12] Exchange Commission of Pakistan, "Exchange Companies Manual CHAPTER 6 GUIDELINES & STANDARDS for ANTI-MONEY LAUNDERING and COMBATING FINANCING of TERRORISM" (), accessed July 17, 2021, https://www.fmu.gov.pk/docs/AML_CFT_Guidelines_in_EC_Manual_by_SBP.pdf.

lone-wolf terrorism making it difficult to find “digital signatures" and use them for further predictions. The paper then says that this problem can be solved by “increasing the size of training datasets” because the smaller size of datasets can only be helpful in crime estimation of minor violations. Algorithms for countering violent extremism need to have already identified terrorists to be successful. Normally it would require intensive investigative work by the authorities to determine the identity and motives of any suspected terrorist.

However, the big data streams carry loads of information about each individual about his digital history. Algorithms allow users to access specific parts of big data to find information about their targets. There are different types of algorithms that are used for various purposes on big data servers. Some allow access to personal information of individuals. Some programs work to explore the financial and travel history. Multiple algorithms can be used simultaneously to explore the entire life of any terrorist including communications with others, financial transactions, travel history and relations with other people. The information of all such aspects is already on big data servers. However, since it is such a big database, algorithms are necessary to extract just the required pieces of information.

The Hadoop cluster system is proposed for combating terrorism efforts around the world. This system uses multiple algorithmic approaches like parallelization, annotators and annotations, lemmatization, stop word remover, term frequency, inverse document frequency and singular value decomposition. This performance has been used in the criminal system in which the experiment's success was determined to be 100%. The success

rate reached 80% in introducing multiple criminal terms with documents. This method also proved effective in node clusters. It can also be used by security agencies in combating terrorism and terrorist activities.[13] The parallelization approach divides a single task unit into multiple units and performs simultaneously on each divided unit. The parallel units are managed by a cluster manager program that increases the processing speed of large streams of data by many folds. Annotators and annotations work by tagging specific documents, images, videos, social media posts, etc. This allows for faster detection of common patterns of communication followed by the terrorists.

Once these terms are identified, the process of lemmatization will then merge the similar terms to establish more specificity. The stop words remover further removes unnecessary words. Term frequency and inverse document frequency define the weightage of the terms that are derived from the search. Singular value decomposition further elucidates the terms that have high weightage and identifies the sensitive terms with 100% accuracy. The proposed method can be a potential source of counter-terrorism efforts. It carries great potential in recognizing the key terms that can be used in analyzing the streams of big data to find out any sort of communication by the terrorists.

[13] Binod Kumar Adhikari et al., "Detection of Sensitive Data to Counter Global Terrorism," *Applied Sciences* 10, no. 1 (December 25, 2019): 182, https://doi.org/10.3390/app10010182.

Along with Algorithms, there are many potential pathways to be highlighted in the field. Following are the some of the significant actions mentioned.

Tracking Money Laundering

The transition of economic markets from analog to digital brought about many changes in financial transactions around the world. It opened new doors for state and non-state actors to go about their businesses. The transfer of money using online platforms leaves a trace of the identity of the person or organization making transaction. Records of these transactions become a part of big data that can be accessed by the concerned authorities. The non-cash payment methods that lead to financial crimes are recorded in big data storage hubs. The various patterns followed in the conduct of illegal transactions are recorded in the database and analyzed by the Financial Intelligence Unit (FIU).

The FIU can use the given patterns to form a typology that highlights the activities of such unlawful operations.[14] The Financial Action Task Force (FATF) is the authority responsible for tracking the illegal activities in financial transactions across all regions. The FATF on Anti-Money laundering is especially active in investigating terror financing and its sources. There is an increasing need to automate the different typologies so they can be used to detect new patterns of money laundering that surface across the world wide web.

Thor Olavsrud recommends automating anti-TBML (Trade Based Money Laundering) monitoring system that is essential for collecting and analysing

[14] Kirill Plaksiy, Andrey Nikiforov, and Natalia Miloslavskaya, "Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism," *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, August 2018, https://doi.org/10.1109/w-ficloud.2018.00017.

external and internal structured and un-structured data. He is convinced such a program should appropriately adjust across key business regions and integrate computerized processes utilizing an assortment of cutting-edge methods, including Text investigation, Web examination, Web-slithering, Unit cost examination, Unit weight investigation, Network (relationship) examination of exchange accomplices and ports, international exchange and nation profiling investigation.

The proposed method of automation will result in the use of the data collected by banks about their customers to form a better track of their transactions. The banks record personal information of all their clients like their name, age, background, businesses or jobs, their financial history and the locations of their transactions. Whenever there is a breach in the financial security or a national security threat is identified, the data gathered is used by the Financial Investigation (FI) that works to form a clear path of the financial movements both in cash and by digital platforms. The formation of history allows for tracking the current pathways of transactions by using the set typologies formed by various data sets.

The findings of the FI then lead to Information Security (IS) branch that further investigates the IP addresses and digital footprints of the transactions. Big Data tools are used to analyze the information obtained by both FI and IS and their resultant observations and hypothesis are then transferred to the law enforcement authorities to act upon. It would be helpful to introduce new methodologies to automate the new generations of variants of money laundering and terrorism financing. The proposed method includes generating new typologies from existing criminal cases to form new variants. The data from these variants can then be analyzed by the big

data tools to detect any unlawful activities of the data sets that are formed as a result of automation.

Games – Modes of Communication

Initially, games were invented for entertainment. What started as a children's plaything is now one of the most dangerous and untraceable modes of communication among the terrorists. There are thousands of online games that have been launched all around the globe and have the feature of online communication in real-time. Belgium's Deputy Prime Minister, Jan Jambon, gave a warning about the secret communications of terrorists over gaming platforms three days before the Paris attacks. He emphasised that communications through gaming systems, including the PlayStation 4 (PS4), are significantly more difficult to monitor than those over social media sites like Facebook or WhatsApp.

The PS4 Network (PSN), provides a party chat function that allows for text and voice communications among players. The feature can also be accessed via mobile phones making it much harder to track and easier to exploit.[15] Jeff Bakalar in an interview with CBSN cited how terrorists can utilize gaming stages to communicate in a tiny space to be gotten catch as the data and correspondence from gaming stations would be encrypted texts, that are difficult to be found. The domain of online gaming goes mainly unnoticed on monitored channels of social media. The difficulty in tracking communications and cryptocurrency transactions in online games provides

[15] Ethan McMahon, "Communicating Terror: The Role of Gaming Consoles and Backdoors," Columbia Journal of European Law, January 15, 2016, http://blogs2.law.columbia.edu/cjel/preliminary-reference/2016/communicating-terror-the-role-of-gaming-consoles-and-backdoors/.

a vacuum where terrorist organizations and other criminal offenders can carry out their businesses without much risk of detection.

The online gaming systems can be exploited mainly for four purposes i.e., content propagation, radicalization & recruitment, communication, combat training and money laundering & terrorist financing. Such terrorist goals can be deterred to some extent by adopting surveillance in online games. The gaming companies should cooperate with security authorities to stop terrorist's efforts on such platforms. During the 2000s, various terrorist groups used online gaming to teach war tactics and influence the minds of young gamers in joining their cause. One such example is a game developed by Al-Qaeda called "Salil al-Sawarem" (The Clanging of the Swords).[16]

Terrorists have also been known to use popular games like world of warcraft for their recruitment efforts and crypto transactions. To put a stop to such transgressions, the lawful authorities need to form algorithms that will alert them to certain keywords used in any online game. The keywords can constitute commonly used words by terrorists in other intercepted communications. Furthermore, gaming companies can also provide security agencies with access to their encryptions which would allow for a quicker breakdown of terrorist communications that can be analyzed via big data tools. The information from games also constitutes a chunk of big data so the algorithms necessary to pick out the necessary parts of the data would need access from the companies.

[16] Ahmed Al-Rawi, "Video Games, Terrorism, and ISIS's Jihad 3.0," *Terrorism and Political Violence* 30, no. 4 (August 5, 2016): 740–60, https://doi.org/10.1080/09546553.2016.1207633.

Following Social Behaviour

Following the social behaviour of a terrorist can be detrimental to recognizing the motives and identities of terrorists all around the world. The use of deep neural networks (DNN) by identifying five key parts of terrorist activity can be used to deter their acts pre-emptively. In the paper "Prediction of Future Terrorist Activities Using Deep Neural Networks" M Irfan along with his colleagues have recognized five distinct variables that are vital to foresee counterterrorism. These variables are regardless of whether the kind of assault is self-destruction, regardless of whether the assault is fruitful, what sort of weapon might potentially be utilized, which locale might conceivably be focused on and what sort of fear monger will be utilized. They have created various models because of conventional Artificial Intelligence (AI) strategies, yet the outcomes have exhibited that these models can't make forecasts with high exactness. They have created NN-and DNN-based models and the outcomes have exhibited that DNN-based models are the most reliable.

The model because of DNN has exhibited over 95% exactness contrasted with other best-in-class strategies in AI. These profound learning-based procedures can help states and police to figure out the variables of psychological warfare and to plan techniques to manage illegal intimidation before a terrorist movement can occur. The components important for predicting a terrorist attack include if the attack is suicide or not, if it is successful or not, the kind of weapon that is to be used, the targeted region and what sort of terrorist will conduct the attack. Various techniques are being developed to focus on these parameters and form DNNs that can potentially predict any terror attacks in a given region before they can happen. Presently these algorithms have not proven to be very successful.

However, the models based on DNN have proven to be 95% more accurate than other neural networks.[17] If more effort is put into the algorithms forming the DNN, the resultant programs may one day be able to predict future terrorist attacks with the highest accuracy. However, a huge data set is required for that purpose which can be collected by accessing confidential information available on the servers of intelligence agencies around the world. Only with the collective efforts of multiple states can such a program be made possible.

Another proposed method of analyzing social behaviour could be to follow the social media patterns of known terrorists. The records of information recorded on big data like the duration of their time on social media apps, their followers, posts, etc. can be used to measure the influence any user has achieved.[18]

Since it is difficult to tackle all social media accounts and platforms, using this method, the profiles of high-level propagandists can be classified into various categories under their influence level. This will help to identify and deal with the most immediate threats first so that major damage can be avoided. The profiling of terrorists would also reveal their locations so stopping propaganda efforts will not be the only reward. The predictive algorithms based on behaviour analysis can also lead to the discovery of unknown terrorists should they follow the patterns recorded in the data sets of social media profiles.

[17] M. Irfan Uddin et al., "Prediction of Future Terrorist Activities Using Deep Neural Networks," *Complexity* 2020 (April 22, 2020): 1–16, https://doi.org/10.1155/2020/1373087.
[18] Cristina Sánchez-Rebollo et al., "Detection of Jihadism in Social Networks Using Big Data Techniques Supported by Graphs and Fuzzy Clustering," *Complexity* 2019 (March 10, 2019): 1–13, https://doi.org/10.1155/2019/1238780.

Psych Evaluations

Realizing the intentions of terrorist agents and stopping them in their tracks is the core element of anti-terrorist operations. The task of terrorist profiling is to separate the terrorist from the common man. It is often found that they are the same person. Big data serves to contain heaps of information about the daily lives of any individual that can access the internet. However, it is difficult for even teams of individuals to go through all that data to find one specific thing. Algorithms help to put that jumbled data into an organized stream that can easily be sifted through by data analytics.

The psychological evaluations of a terrorist mindset can help to identify them from their behaviour. This sort of data is hard to come by but can be extremely useful in the threat profiling of an individual. Multiple data sets containing profiles of various terrorists are uploaded to an algorithm that runs pattern recognitions from those data sets onto the information available in big data servers. The information from these data sets helps to identify individuals that can be a possible threat. The data sets become the basis of recognizing patterns from real-time data including personal information of each known terrorist like their name, age, emails, phone calls and travelling history etc.[19]

The psychological profiling of a terrorist is difficult because there is a lack of sufficient effort to understand his behaviour. Though there is much data to be found on speculations of terrorist motives, there is little or no information about the inner workings of the terrorist mind. The reason is that there are hardly any terrorists that would willingly participate in a control group to profile their motives. Also, different organizations have

[19] https://link.springer.com/article/10.1007/s11948-020-00254-w#Sec2

different ideologies and various goals which affects the mind of different terrorists in different ways. The data gathered from big data can give a certain viewpoint into the lives of various terrorists that can in turn reveal their motives and indifferences towards each other and the world. It is speculated that psychological profiling can be the greatest asset in pre-empting terrorist attacks should it become possible. The use of big data in establishing parameters of the judgment of the psychological mind of a terrorist can be a huge leap in that direction.

Geo Tag Devices

Geo-tag devices have a global positioning system (GPS) integrated into them that can send the coordinated location of anything they are tagged in the form of a message or an image. In the contemporary era, geo-tag devices are used in cars to keep a track of their movements in certain areas. These are mostly implanted by banks when they loan out a vehicle or by the police when they need to run surveillance on a suspect. The geotag devices are directly linked to GPS satellites. The link allows for tracking the real-time location of anything that is tagged with the device. It is also possible to tag online posts on digital social platforms.

In 2014, a person from New Zealand who moved to the Islamic State (IS) and tweeted some posts that were geotagged. He later realized his mistake but not before giving away his location. This technology can be used to track terrorists across any region. Their locations in real time could lead to their contacts in a state and reveal their plans of action. The information obtained from geotags can be instrumental in verifying suspects. Counter-terrorism authorities have revealed that geotags provide a lot of information about suspected individuals.

Though they are currently in use, geotags can further be improvised into identifying the unknown enemies as well. The use of geotags along with predictive algorithms that are provided with established data sets to predict new sources of communications among terrorists can potentially allow for the discovery of the exact locations of terrorist groups. Geotags can also be used to keep a track of propaganda efforts on social media. They can be programmed to search for specific keywords or images using the Hadoop cluster system to automatically remove any malicious content that can influence the minds of the young generation.

Emotion Recognition System

Machine learning and face recognition software has long been in use in both domestic and international affairs. They have now become so common that even mobile phones carry facial recognition security systems. Now, along with facial recognition, there is also development in the emotional recognition of an individual. Although the US has been working on this technology for a long time and has had a great measure of success. China has also been in the works to obtain this technology for quite a while. Recently, they have been successful to an extent where they could even take the lead over the US. The Chinese systems have been able to detect the emotions a person is feeling with up to 95% accuracy.

They are of the view that their technology can have unrivalled uses in both military and non-military domains. In 2018, the Alpha Eye of China was able to point out a trained sniper from eight soldiers by observing their expressions. This was done at a pace higher than even the most trained

physicians.[20] It is theoretically possible to use this technology to recognize terrorists to catch them in the act. Many suicide bombers and newly trained assets of terrorist organizations show signs of emotional distress when on a mission. Their psychological profiles along with the emotional detection programs can, to a great degree, work to prevent terrorist attacks on a global scale.

Such measures implemented in states across the globe will raise a lot of questions about the privacy of individuals, however, it is a necessary sacrifice for greater security. The emotion recognition systems should make use of security and traffic cameras around important structures to establish emotional profiles of individuals seen in the cameras. Any suspicious individual would soon be apprehended and questioned by the authorities. This model will take a lot of time and effort to be implemented. Initially, a lot of issues can arise about false positives and the inflow of stressful individuals. For this purpose, various data sets would have to be introduced in programs after they have been installed to keep the focus on individuals that can harm civilians. But, the benefits of such a program are every bit worth the effort as the rewards could potentially bring peace to entire regions.

Access to Local Departments

Since big data is just a muddle of information that spans over yottabytes, there are not many systems that can effectively access it. Even among major tech companies, there is only a select few that can access more than a few domains of big data as it requires a huge amount of processing power. For

[20] Huang Lanlan and Lin Xiaoyi, "China Leads in Emotion Recognition Tech, Reinforces Privacy Rules to Tackle Abuse - Global Times," www.globaltimes.cn, 2021, https://www.globaltimes.cn/page/202103/1217212.shtml.

instance, iTech Art is a company that specializes in Artificial neural networks in big data. They also excel in AI algorithms and applications, big data cluster management, parallel processing and GPU processing. IBM keeps its focus on the Hadoop system, Stream computing and Federated discovery and Navigation.[21]

Therefore, the access to the servers of big data is restricted in the law department to intelligence agencies or those dealing with national threats. Since there is a lack of necessary processing power in the official servers of government agencies, they cannot afford unrestricted access to bug data that hinders their abilities to perform their jobs. However, it should be possible to provide access to a few smaller data sets of big data to local law enforcement agencies as well.

The local authorities can use such data sets to run the light predictive analysis, emotion detection, facial recognition and pattern analysis on any given suspect to make quick judgments. This could help them to recognize and effectively deal with the already known threats. It takes some time for local agencies to contact the higher authorities for access upon suspicions about an individual or a group. This hassle can be avoided if local departments are provided with a degree of access that can be managed. It will increase their chances of apprehending terrorists before they can get a shot at implementing their plans.

The local agencies would also have to sign agreements to misuse not the given access. There are a lot of suspicions of corruption and fraud among

[21]Software Testing Help, "Top 13 Best Big Data Companies of 2019," Softwaretestinghelp.com, November 20, 2019, https://www.softwaretestinghelp.com/big-data-companies/.

the local law enforcement authorities by the people. The governance system will have to ensure that the data access will not compromise the integrity of the citizens in any way. It would go a long way in establishing trust with the civilians if the inappropriate access to their information from big data servers was made punishable by law. The cooperation of the public is just as necessary in maintaining national security as in the establishment of law enforcement agencies and courts to ensure social justice.

Dark Web Tracing and Blockage

The dark web is a part of the internet that is not accessible to the public. Some specific requirements have to be met to access that platform. Even if someone manages to access the web, the workings of the system are too complex for any common man to understand. It is imperative to make sure to hide one's digital signature before entering the dark web as it is extremely easy to track someone who is not using the proper equipment for hiding his identity.

The encryptions that are used by professional hackers and terrorists on the dark web are too complex to track. This is because the dark web covers most illegal markets and trade agreements. It is believed that many of the world's elite personalities use the dark web to gather things like artwork, drugs, machines etc. that would normally be inaccessible to the public. It is also possible to get fake identification documents and weapons. The promise of anonymity along with access to all sorts of unique and illegal goods make the dark web alluring to anyone looking to carry discreet transactions. Terrorists have also been known to use the dark web for communications, propaganda and weapons deals.

They possess the necessary hardware to mask their signature on the digital domain on the dark web. Therefore, the law enforcement agencies are left with no other choice but to access the dark web themselves to follow the communication pathways of terrorists. This approach, however, can only work if it is known when the terrorists are communicating and what IP they are using for their messages. That is why it is not a very successful way of countering terrorists as often there are decoys found among the intercepted communications that are extremely misleading for the authorities.

One way to overcome this situation would be to form algorithms that can detect subtle changes in the changed IP addresses that are formed using external hardware. Should this become possible, it would change the whole dynamic of the dark web as anonymity would no longer be guaranteed. This could not only disrupt the illegal trades and transactions over the dark web but could also lead to the discovery of established and potential terrorist hideouts, the revelation of their attack plans and the locations of the sleeper cells etc. The ability to track the real location of the user of the dark web could provide us with the data sets to unravel multiple encryptions on the dark web.

Dividing National and International Communication Platforms

Social media provide a great attraction for people of both young and old generations. The influence has expanded to such an extent that life without it seems unimaginable for the younger generations. Terrorists also use social media to send their propaganda messages across the borders and into the world. Despite efforts from multiple companies and authorities, the social media accounts of terrorists are active on many platforms. Since major

social media platforms are utilised by people around the world, terrorists will find it easier to direct their propaganda efforts towards masses at once.

This can be avoided by launching social media applications separately for national and international use. The national applications can focus on the people of a state that can have no outside interference. The propaganda launched on such platforms would tell us that there are terrorists within the state and their locations can become relatively easier to trace. The option of hiding the identity by using a VPN would still be available but the impact would be greatly reduced as it would become easier to identify posts from outside sources.

International applications should be launched separately where people can interact with each other on a global scale. The global applications should be completely accessible by the governing authorities without any data restrictions so they may be able to monitor any terrorist chatter on such platforms. The posts on such platforms would be harder to track but also less likely to influence the minds of young people once they realize that they cannot be trusted. There is the possibility of hiding the digital signature to access anonymous servers, however, if the algorithms to track the activity on the dark web become a reality, then they can be utilized in such applications to break the multi-layered encryptions that hamper the detection efforts of intelligence agencies. The implementation of such a system will be met with much hostility, especially from the younger generation that has become increasingly dependent on social media in their daily activities. But that has also made them susceptible to dangerous suggestions from terrorist propaganda. Ultimately, it will be up to the

people how they choose to reach the information provided to them, but this system can help them to better identify who the real enemy is.

Conclusion

Cyberspace is considered to be a complicated domain in state affairs as it does not have any physical parameters for control. Unlike the other domains of land, sky, sea and outer space, cyberspace exists in a virtual plane and is easily accessible by all individuals around the world. The new time of worldwide extremist warfare has carried new difficulties to which the speed of progress in counterterrorism practice has been phenomenal in the world's long history of safeguarding the safety of respective states.

This paper investigates the need for inventive ideas, distinguishing the analytical difficulties of taking care of expanded volumes of data, considering new functional difficulties from arising dangers and inspects how Big Data can quickly foster counterterrorism practices to speed up the ID of terrorist organizations, support recognizable proof of the underlying foundations of radicalization inside web-based networks and increment the adequacy of counterterrorism procedures to protect residents from the contemporary threat of terrorism.

This is not practically possible to achieve enduring success through big data only, it is mandatory to have a combination of both Human intelligence and big data analytics. Tasks for examiners arrive when the data is collected and now, they have to analyze it to other levels to get a realistic view of changing nature of situations and that too is demanding. Specifically, in circumstances where oppressors are trying hard to misuse and manipulate the platforms that are the source of the information that is to be analyzed by officials.

A large amount of data is to be considered again and again for better results. So the combination of Human intelligence and big data is mandatory to achieve the desired results of peace maintenance whether in a specific state or globally. Different cyber-attacks and physical assaults have brought the security agencies to use big data in finding the clues to offenders and offences. From the ascending amount of data, security officials have infused largely in the artificial intelligence and technologies to gather and analyze data. Even though the expertise of agencies lacks in dealing with a huge amount of data, the security departments still try their level best to analyze and excel in their managerial capabilities with the help of big data.

Although the process of extracting useful information from this exponential amount of data is tough and crucial, still agencies are somehow successful in the race. So the use of big data for combating violent extremism is not too futuristic and even some countries are already on the path. We can predict the success and complete elimination of terrorism under the umbrella of big data.

Ms. Maryam Baloch *has done master's in International Relations from National Defence University and is currently enrolled in a short course from LUMS in Cyber security Fundamentals. She can be reached at* ***maryambaloch1281@gmail.com***