# Utilisation of Artificial Intelligence in Fighting Terrorism in Jammu and Kashmir

**AS CHONKER**

## The Power of AI

A unique period of developments in Artificial Intelligence (AI) has seen algorithms with powerful predictive abilities used daily in applications ranging from stock trading to targeted marketing. These technologies may also be translated to the realm of public safety, specifically in predicting terrorist activity or individual involvement in terrorism. A counter-terrorism policy is required to strike a balance between providing security and respecting individual right and liberties. These often conflicting ends must be met from limited resources. Accurate predictions by AI could help direct these resources most effectively. They might also have potential to minimise unnecessary intrusion on the majority of the population and mitigate human bias in decision-making. Conversely, there may be risk associated with rushing to deploy naïve technologies as algorithms can exhibit inherent or learnt biases of their own and be vulnerable to adversarial action.

Following the succession of terrorist attacks and the expansion of terrorist organisations around the world, it has become necessary for anti-terror forces to develop new and more effective solutions that can prevent attacks, identify suspects, react to the moment, and also speed up investigations. In this case,

technology can help protect against terrorism.[1] Artificial intelligence tools are being extensively deployed in an effort to stop terrorists, which include innovative cameras to track suspects, image matching algorithms to match suspects on user-uploaded photos and videos with publicly known terrorist faces, in addition to intelligent sensors to read the iris of every traveller and avoid false identities.

**Terrorist organisations have successfully used social media tools to recruit, propagate and raise funds for their activities.**

## Tools of Terror in J&K

An article in March 2018 had highlighted the importance of understanding the tools of terror in Jammu and Kashmir (J&K).[2] To understand the power of AI in combatting terrorism, it is important to understand these tools. Terrorist groups' activities in J&K can be divided into two interrelated categories: activities that sustain the group's existence as a cohesive entity and activities that allow terrorists to sustain a series of successful attacks. The ability of terrorist groups to sustain a series of successful attacks can turn this success into a recruitment campaign or use the success to reinforce their members' confidence in the group and, hence, bolster group cohesion. In the event of terrorist attacks, social media postings can serve as a force multiplier and accelerator that can amplify the carnage and spread anxiety and fear beyond the immediate victims of a terrorist attack. There is currently no reliable machine learning technology, sentiment analysis software or artificial intelligence programmes that can monitor and vet all content in real-time. The probability of false positives is high when utilising this technology. As a result, time-consuming human analysis will be necessary to filter out false positives.[3]

Terrorist organisations, over the years, have successfully used social media tools to recruit, propagate and raise funds for their dreadful agendas. Sermons by so-called charismatic extremists have succeeded in influencing youths to join terrorist organisations and carry out sinister attacks across the world. One of the key reasons behind the heavy use of the mass media is because ultimately these anti-social elements are trying to legitimise their unlawful activities, as most of them have a mass following online, and the possibility of gaining an even larger audience.[4]

## AI to Tackle Organisational Tools of Terror

- **Ideology and Alienation through Radicalisation:** With regards to terrorism, the term ideology means the consensus of grievances and objectives that a terrorist group is trying to address through violence. In this context, terrorists'

ideologies may take on many forms—e.g. religious or political—but still serve the same purpose—motivating actions, unifying members, and linking the organisation to the communities for which it purports to fight. In Kashmir the ideology is different for different groups. While the Hizbul Mujahideen (HuM) is basically fighting for a Kashmir which comes under Pakistan, the Lashkar-e-Taiba (LeT), Jaishe-e-Mohammed (JeM) and now Islamic State of Iraq and Syria (ISIS) off-shoots seem to have more religious lineages with the ultimate aim of merging with Pakistan, or the Caliphate in the case of the ISIS. Thus, the ideology is a mix of ethno-religious separatism and Islamic extremism. Although the sense of alienation from the Indian mainland is present in the *awam* due to many other reasons like cultural differences, historical baggage and dysfunctional governance, it is a well-known fact that state sponsored militancy has dramatically transformed the Sufism and Kashmiriyat influenced people of Kashmir into a fractured and radically influenced society which, in turn, has given rise to religious fundamentalism.[5] Radicalisation of society in Kashmir feeds the further alienation of the people,[6] which is the aim of the terror groups and it seems to be the first step for gradually bringing the youth into the main line of militant actions. Online radicalisation has become a bane for law-makers across the world and has gradually become the biggest source for radicalisation. We could take a leaf out of the UK Home Office which has successfully encouraged the large online content platforms to invest in automated detection technology that can spot and remove radicalising videos. However, the videos remain available on a large number of smaller video hosting platforms, which do not have the AI expertise or the resources necessary to develop their own detection capabilities. Collaborating with the UK Home Office Counterterrorism Unit, ASI Data Science has built a tool that removes extremist propaganda from the web.[7] The new technology is capable of detecting 94 percent of the ISIS' online propaganda with 99.995 percent accuracy. Any content that the software is still unsure about would then be passed on for a human to review.[8] The goal is to stop the majority of video propaganda before it ever reaches the internet.

- **Leadership:** In insurgency and terrorism, terrorist groups tend to coalesce around charismatic individuals who attract and inspire supporters. There are many terrorists who are more than willing to get into the shoes of a slain leader. Power and money will always have takers. A strategy to take on the leaders will definitely give an operational advantage, however, in the longer run, slain terrorist leaders also provide a grander sense of martyrdom for the

cause to the youth, which motivates others to take on the cause, a case in point being the Burhan Wani incident. Hafiz Saeed and Maulana Azhar are Pakistan state sponsored rogues but Syed Sallauddin is one leader who has the potential to be won over as he himself had taken part in elections and his group had earlier agreed to a ceasefire. While, on the one hand AI can effectively eradicate video propaganda on the internet, it can also be utilised effectively to win over potential turncoats by automatically replacing terrorist propaganda with appealing stories and videos by boosting other sites.

- **Recruitment:** In the Valley, there is an adequate pool of disgruntled, unemployed youth, both educated and uneducated, for recruitment by anti-national elements. Typically, a strategy of systematic entrapment is employed whereby individuals are instructed to undertake operations that are progressively more serious in nature. The objective is two-fold: first, to induce inductees to greater acts of disobedience and violence; and second, to slowly distance these individuals from mainstream civil society to the point that they have no real option but to remain with the militants. In most cases, the procedure seems to follow a standard pattern that starts out with the youth being used to target the Security Forces (SFs) via stone pelting for money, progressing through more serious vandalism and then being an Over Ground Worker (OGW) wherein he provides logistical support for strike teams, before he joins the mainstream groups for more serious actions. AI could be utilised effectively to monitor and carry out statistical analysis of the whereabouts of the offenders at various levels to draw patterns which could lead to the recruiters.
- **Publicity:** For the insurgents, the need to win over the population is being reflected in their perceived conduct of operations which have very limited collateral damage. The propaganda strategy of the terrorists here stems from their perceived actions of avoiding civilian casualties while, at the same time, capitalising on the mistakes of the SFs. The terrorists have managed to not only identify themselves as freedom fighters but have also been portrayed as fighting for *jihad*, both factors which provide them the unconditional support of the population. The mainstream media is also creating a perception that the terrorists are winning ground. AI tools can be utilised to carry out continuous statistical analyses to highlight the collateral damage that the terrorists and their handlers are effecting by their involvement of innocent youths of the state in their unjust cause.
- **Finance:** The terrorist organisation can only sustain its operations if there are adequate means to generate funds for the cause. Rerouting the *hawala* funding

from Saudi Arabia, Iran and the Kashmiri diaspora seems to be primary means of funding. Notably, the terrorist organisations in both Pakistan Occupied Kashmir (POK) and the Valley do not use these resources solely for their terrorist operations but also sponsor a number of charities in the POK. Thus, it is difficult to separate the funds the organisation uses to support health clinics from those used to support terrorist activities. Therefore, although money is the key for a terrorist organisation to sustain its activities, it also plays an organisational role—group cohesion—by bolstering its relationship with the local communities and further legitimising its activities in J&K. The balance of payment in the Line of Control (LoC) trade and narcotics, Haj tourism cancellations as well as sale and distribution of ancestral property assets between families on both sides of the LoC seem to be the new sources of financing the movement in the Valley. A new trend yet not fully discovered and investigated is the Hurriyat and Pakistan sponsored 'scholarship scandal' wherein students are being sent to the South Asian Association for Regional Cooperation (SAARC) and other countries, thereby financing terror in kind. Banks have long used anti-money laundering systems to flag suspicious activity,[9] and they have turned to those same legacy tools to catch terror-related transactions, too. But these legacy tools are not up to the job. If the software spots a seven-figure transfer of funds from Dubai to Srinagar, for example, it knows to flag it. But as terrorist groups like the ISIS and JeM recruit people internationally for smaller, targeted attacks, those tools become far less effective. The pattern of small transactions that a terrorist in hiding makes might not raise red flags for the usual anti-money laundering systems, unless those systems use AI. Banks are increasingly turning to machine learning to mine vast quantities of bank data and find anomalies in accounts and transactions that might otherwise have gone unnoticed. It is a surgical approach to finding a needle in a haystack. AI technology can be used to identify money laundering, terrorist funding, and other financial crimes. The challenge, particularly for banks looking to stop the flow of money to foreign fighters, is that there are infinite possible permutations of transactions. A person looking to join the ISIS, Al Qaida or HuM might take $80 out of an ATM in Brussels, receive a wire transfer in Algeria, use a credit card in Lebanon or open an account for money transfer in Srinagar or send money home. On their own, these incremental activities may not trigger suspicion, but taken together, they create a pattern that a machine might identify as suspicious. Of course, as with any computer system that can learn on its own, the results are only as good as the data fed into it, and the human oversight and controls put

on them. As human beings slowly adapt to the sneakily ubiquitous threat of terror in our own lives, machines will need to adapt even faster to help choke it off.

**Monitoring of big data through AI enabled tools could provide details of terrorist congregations.**

## AI to Tackle Operational Tools of Terror

- **Command and Control:** In the initial stages of the insurgency in the Valley, a hierarchy of mid-level leaders met periodically to formulate basic strategic guidance, allowing the leaders discretion in the way that they achieve their overall objectives. This network was facilitated by a system of radio transmitting stations. The capability of interception and breaking of codes by our forces led to reduced usage of radio communication. This had severely hampered the command and control set-up in the Valley. However, of late, the terrorists seem to have shifted to sophisticated methods of communication, including the internet to transmit messages. Social media has a terrorism problem. From Twitter's famous 2015 letter to the US Congress that it would never restrict the right of terrorists to use its platform, to its rapid about-face in the face of the public and governmental outcry, Silicon Valley has had a change of heart in how it sees its role in curbing the use of its tools by those who wish to commit violence across the world. Facebook released a new transparency report that emphasizes its efforts to combat terrorists' use of its platform and the role that AI is playing in what it claims are significant successes.[10] Yet, that narrative of AI success has been increasingly challenged, by academic studies suggesting that not only is content not being deleted, but that other Facebook tools may actually be assisting terrorists, to a Bloomberg piece that demonstrates just how readily terrorist content can still be found on Facebook.
- **Weapons and Equipment:** Notwithstanding the fact that there is an adequate quantity of weapons hidden in the Valley, more still seem to be coming in. Use of AI enabled 3-D vehicle CT scanners at entry points as well as robots to monitor and report ingress without the involvement of the human angle are some AI keys to ramp up security.
- **Operational Space and Security:** Terrorist groups need time and space to plan, train for, and execute, their attacks. The operational space will range from urban neighbourhoods to sanctuaries within the state and transnational sanctuaries to plan, train, and conduct operations, stockpile weapons, and protect their primary leaders. These areas could be traditional hideouts like the Lolab

and Rajwad Radio Frequency (RF) or places like Srinagar downtown, Sopore downtown or Pulwama town, where the density of population and houses makes it extremely difficult to conduct operations. Operational space for each terror cell in terms of a jurisdiction or territorial limitation, seems to be clearly demarcated by their handlers. Monitoring of 'Big Data' through AI enabled tools could give a fair idea of terrorist congregations and whereabouts in order to bust these hideouts/training areas. Terrorists expend considerable resources to protect the integrity of their operations, thus, switching to a cell-like structure to maintain operational security to operate relatively independently. Terrorist groups have also switched to sophisticated methods like encrypted software. Launching of indigenised AI enabled apps or AI enabled data mining of on-shore servers could help in breaking the code.

- **OGWs:** Overground workers have always been the mainstay of an insurgency movement. Previously, the OGWs were primarily involved in logistics support and intelligence gathering. Of late, the distinction has blurred considerably, with OGWs also capable of carrying out small scale strikes while retaining the capability to mix rapidly with the population. Sympathisers, in the form of teachers in educational as well as religious institutes, are corroding the minds of children, and instigating them to join the militancy. Funerals of slain militants have become the new hot-spots of recruitment by OGWs. AI enabled drone-borne cameras and at checkpoints as well as at public places, could help in monitoring and stinging these OGWs who are fuelling the fire in young minds.
- **Cyber Space:** Groups like Al Qaeda, LeT, and ISIS have successfully created online *madrassas* that have made a significant dent in the young and vulnerable population across the world from the West to the East, and irrespective of their religious inclination. They have also succeeded in gathering massive 'sympathisers' online. Despite the knowledge about the social media, platforms like Twitter, Facebook, Google, YouTube, WhatsApp, Skype, Tumblr and Instagram owned by the US corporations have been misused by the terrorists. To this end, Facebook is developing "text-based signals" from previously removed posts that praised or supported terrorist organisations. In this unique undertaking, those signals were fed into a machine learning system, which, over time, will learn how to detect similar posts. Similarly, Google is targeting hateful content with machine learning-based systems working with human reviewers and Non-Governmental Organisations (NGOs) in an attempt to introduce a nuanced approach to censoring extremist media.

- **Agitational Space:** Although the term "agitational terrorism" was first coined in 2009,[11] the effect of it has been seen mainly since the Burhan Wani incident wherein organised stone pelting mobs stopping the proceedings by the security forces at an encounter spot have almost become a norm. The organisational tools of finance and alienation through radicalisation have a deep connect for successfully employing this operational tool. AI tools for fighting these two organisational tools could be utilised to put an end to agitational dynamics.

## Conclusion

During a recently concluded research in the Centre for Land Warfare Studies (CLAWS), AI was utilised in conjunction by a student of Carnegie Melon University, USA, in order to analyse data collected from the students in colleges in Kashmir through a questionnaire designed by the Tata Institute of Social Sciences. Some of the major findings of this exercise are given below:

- Trust on the Indian armed forces deployed in Kashmir seems to be most highly positively correlated with the sense of being Indian, across all the three major geographical regions of the Kashmir Valley. This is expected, since the Indian Army has played an active role in fighting armed militancy and also undertaken numerous civic action programmes.
- Trust on the local and police agencies seems to not be correlated with this sense, suggesting an opportunity for the local police to take up similar civic action programmes to reach out and play a more active role in creating a nationalistic and democratic sense of belonging to the Union of India.
- Interestingly, a large number of participants responded that the primary purpose of social media was to express opinions, and a political dialogue also had a positive disposition towards the Indian Union. This suggests that social media, although infamous for its deleterious effects in the Valley, does provide a platform for the youth to engage in political discourse, encouraging state instruments to play a more active role through it for positively engaging the population through these media.
- Amongst the population, with a general lack of trust on the Indian state and its instruments, such mistrust extends to even other non-state instruments, including the private electronic media.
- The effects of both traditional and social media seem to be positively correlated with the responders' age too, which is contrary to public opinion about social media being more popular with the younger population.

- While one would expect this to be the case for the electronic and print media, the fact that the influence of the social media on separatism seems to increase with age is an interesting discovery and it could point to the negative role being played by some teachers in educational institutes. AI assisted pattern reading of the disciples in their future actions could lead us to the errant teachers involved in the radicalisation of society.

The benefits of AI technology to fight terrorism are infinite, however, scientists are facing a critical paradox: the terrorists themselves could use these same technologies. Imagine a terrorist organisation utilising drone-borne facial recognition and Improvised Explosive Devices (IEDs) for political assassinations. Therefore, it is essentially a race for innovation which requires a more proactive approach. Rather than adapting technologies to stay ahead of evolving dangers and changing tactics, they need to be ahead of the terrorists and develop "overmatching" security systems that protect the public, safeguard their freedom, and leave travel and commerce unaffected.

---

Col **AS Chonker** is presently a Senior Fellow, CLAWS.

## Notes

1. https://www.leyton.com/blog/?p=1893-leveraging-ai-machine-learning-techniques-fight-terrorism, Accessed on December 3, 2018.
2. http://www.claws.in/images/publication_pdf/1027785870_Cissuebrief.pdf. Accessed on December 3, 2018.
3. https://qrius.com/terrorism-social-media, Accessed on December 4, 2018.
4. www.dailyexcelsior.com/social-media-and-terrorism, Accessed on December 4, 2018.
5. http://www.claws.in/images/publication_pdf/ Psychological Aspects in Kashmir: Why Kashmiriyat Has Won Against Haivaniyat=ASChonker(Final).pdf. Accessed on December 5, 2018.
6. Ibid.
7. https://conferences.oreilly.com/artificial-intelligence/ai-eu/public/schedule/detail/70263, Accessed on December 6, 2018.
8. https://i-hls.com/archives/81392, Accessed on December 6, 2018.
9. https://www.wired.com/story/quantaverse-ai-terrorist-funding/, Accessed on December 8, 2018.
10. https://www.forbes.com/sites/kalevleetaru/2018/05/15/the-problem-with-using-ai-to-fight-terrorism-on-social-media/, Accessed on December 10, 2018.
11. http://www.satp.org/satporgtp/sair/Archives/sair8/8_35.htm, Accessed on December 12 2018.