DEFENCE AND DIPLOMACY

IN PURSUIT OF NATIONAL SECURITY

VOL. 12 NO. 3 ISSN 2347 - 3703 APRIL-JUNE 2023

JOURNAL OF THE CENTRE FOR AIR POWER STUDIES

THE IMPACT OF SOCMINT ON COUNTERTERRORISM

PRIYADARSHINI BARUAH

In November 2022, a pro-Islamic State of Iraq and Syria (ISIS) Telegram account encouraged its followers to carry out terrorist attacks at the 2022 FIFA World Cup, hosted by Qatar. Messages in the account urged ISIS supporters to take this event as a 'golden opportunity'[1] to carry forward what they call their fight against the *Kafirs*, be it in the form of biological or any other form of innovative attack. It is important to note that similar threats to carry out attacks were made by ISIS and its sympathisers even during the 2018 FIFA World Cup, hosted by Russia, but nothing unfortunate occurred. However, the Wafa Foundation, a media unit of the ISIS, used an image of Lionel Messi[2] to send terror threats during the 2018 FIFA World Cup. ISIS has set up the trend of using the FIFA World Cup

Ms **Priyadarshini Baruah** is Research Associate at the Centre for Air Power Studies, New Delhi.

1. "Pro-ISIS Telegram Channel Threatens Attacks at FIFA World Cup Qatar 2022, Encourages Biological Attacks, Provides Telegram Account to Connect to Obtain Biological Substances", *MEMRI Jihad & Terrorism Threat Monitor*, November 7, 2022, at https://www.memri.org/jttm/pro-isis-telegram-channel-threatens-attacks-fifa-world-cup-qatar-2022-encourages-biological. Accessed on May 13, 2023.
2. "Pro-#ISIS media unit Wafa' Foundation continues to threaten 2018 FIFA #WorldCup, this time using an image of #Lionel Messi in a prison outfit", SITE Intelligence Group (Twitter Account), October 24, 2017, at https://twitter.com/siteintelgroup/status/922863797928329216. Accessed on May 13, 2023.

platform to propagate their doctrine. The height of the ISIS trend of hijacking occurred during the 2014 World Cup. They made use of the hashtag "#WorldCup2014". Instead of football, all tweets under this hashtag became synonymous with ISIS.[3] This indicated that the trend was hijacked by ISIS supporters and their bot accounts.

ISIS, also known by its Arabic acronym Daesh, is an offshoot of Al-Qaeda. Although it began in West Asia, it has now extended its tentacles to most parts of the world through its offshoots like the Islamic State-Khorasan Province (ISKP), active in Afghanistan. This group is a radical militant organisation whose focus has always been on building a proto-state (new caliphate). The organisation employs social media as a strategic tool for promoting its message and recruiting globally. In addition, this group is well known for uploading various Jihadi propaganda content on the internet.

According to *The Spotlight on Global Jihad* in its April-May 2023 edition, "Intelligence agencies have issued warnings regarding the initiation of an ISIS recruitment campaign targeting technologically skilled young individuals in India, primarily focusing on youths from the Indian states of Karnataka and Rajasthan. Intelligence sources indicate a recent surge in the number of Indian youth becoming radicalised and affiliating themselves with ISIS."[4] *The Tribune* has recently reported that "In December 2022, a security source in India reported that 21 radicalised individuals had joined ISIS. Subsequently, the numbers increased in subsequent months, with 28 individuals joining in January 2023, 37 in February 2023, and 36 in March 2023. The recruitment process is facilitated through online platforms, with ISIS utilising the Dark Web Academy to provide radicalisation and training for engaging in terrorist activities. Intelligence sources further suggest that a group called *The Transparent Tribe*, targets collecting data from universities by hacking and online theft, these information are then disseminated to various terrorist organisations,

3. "The Command of the Trend: Social Media as a Weapon in the Information Age", The School of Advanced AIR and Space Studies, AIR University, June 2017, at https://www.hsdl.org/?view&did=805404. Accessed on May 13, 2023.
4. "ISIS activity in India", *Spotlight on Global Jihad*, April 24-May 10, 2023, at https://www.terrorism-info.org.il/app/uploads/2023/05/E_086_23.pdf. Accessed on May 13, 2023.

including ISIS."[5] Terrorism and social media have had the largest expanding influence on human existence over the last decade. In this technological era, terrorist organisations rely extensively on open media networks in democratic nations to communicate their message and aims.[6] Terrorist organisations resort to acts of violence and hostility against people in order to gain attention for their cause. This strategy has proved to be a success in attracting attention.

This article aims to understand the concept of Social Media Intelligence (SOCMINT) along with its benefits and limitations. It further aims to assess the role of social media in gathering intelligence, focusing on how it makes posting information online easy, understanding the strategy, recruitment and expansion, modus operandi of terrorist organisations and public opinion.

UNDERSTANDING THE CONCEPT OF SOCMINT

SOCMINT implies a collection of various instruments and solutions that allow organisations to analyse conversations, respond to social signals, and produce social data points based on the needs of the users. These are then converted into trends and analyses that are considered meaningful by the user. Some analysts have suggested SOCMINT to be an element of what is known as Open-Source Intelligence (OSINT), and it is described as "information that is available publicly and may be lawfully accessed by either request, purchase, or observation".[7] Through both intrusive or non-intrusive means, and from open and closed social networks, SOCMINT permits one to gather and utilise intelligence from various social media sites. Open SOCMINT is the type of SOCMINT that is believed to be useful and important in counterterrorism and public safety efforts.[8] The term SOCMINT was

5. "ISIS eyeing techies from India: Intel", *The Tribune*, May 8, 2023, at https://www.tribuneindia.com/news/nation/isis-eyeing-techies-from-india-intel-505774. Accessed on May 13, 2023.
6. "Terrorism and Social Media", Indian Institute of Legal Studies, July 31, 2021, at https://www.iilsindia.com/blogs/terrorism-social-media/. Accessed on May 2, 2023.
7. Florian Schaurer, "Social Media Intelligence (SOCMINT)—Same Song, New Melody?", Open Source Intelligence Blog, October 31, 2012, at https://osintblog.org/2012/10/31/social-media-intelligence-socmint-same-song-new-melody/. Accessed on May 2, 2023.
8. Jamie Bartlett and Carl Miller, "The State of the Art: A Literature Review of Social Media Intelligence Capabilities for Counter Terrorism", Demos, November, 2013, at https://demos.co.uk/wp-content/uploads/files/DEMOS_Canada_paper.pdf. Accessed on May 2, 2023.

first used in 2012 by Sir David Omand, Jamie Bartlett and Carl Miller in a co-authored study, "Introducing Social Media Intelligence".[9] Even though the paper focused on social media as an integral part of intelligence and security, it is argued that analytical, regulatory and technological changes are required before considering social media as a powerful tool for gathering intelligence.

The use of social media has grown extensively in the Intelligence Community (IC). Back in 2016, in-Q-Tel, the Central Intelligence Agency's (CIA) venture capital fund, reportedly invested in many technological firms that are capable of gathering and analysing social media data to detect aberrations.[10] These investments, in particular, give people danger scores based on their online speech. Although it was first published in 2016, it is widely assumed that the CIA has been collaborating with such companies for years, incorporating SOCMINT into normal analytical schedules. Many other companies have claimed similar capabilities, and both private and public sector organisations have been heavily researching methods to both monitor and interpret online behaviour on these platforms, as well as methods to identify warning behaviours online before people become tangible threats. This form of online predictive analysis has been favoured by the Defense Advanced Research Projects Agency (DARPA), as well as by the law enforcement agencies and police forces.[11] Along with them, others have also recognised social media as a unique approach to identify behavioural trends online while also predicting future individual behaviour. The rationale behind the aforementioned investments and objectives is not unexpected, considering the advantages that information gathered from social media can help the Intelligence Community and law enforcement, in addition to the

9. Sir David Omand, Jamie Bartlett and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)", *Intelligence and National Security*, December 2012, pp. 801-23, at https://www.researchgate.net/profile/David-Omand/publication/262869934_Introducing_social_media_intelligence_SOCMINT/links/5703ebaf08ae74a08e245b3c/Introducing-social-media-intelligence-SOCMINT.pdf. Accessed on May 2, 2023.
10. Tom Risen, "CIA Tech Firm Seeks More Social Media Spying", US News, April 15, 2016, at https://www.usnews.com/news/articles/2016-04-15/cia-tech-firm-seeks-more-social-media-spying. Accessed on May 2, 2023.
11. George Leopold, "DARPA looks to tap social media, big data to probe the causes of social unrest", *Defense One*, March 11, 2016, at https://www.defenseone.com/defense-systems/2016/03/darpa-looks-to-tap-social-media-big-data-to-probe-the-causes-of-social-unrest/189008/. Accessed on May 2, 2023.

efficacy of such surveillance practices. The collection and analysis of social media data can generate valuable insights into the personal details, beliefs, and behaviours of individuals and groups, which can aid in the identification and mitigation of potential threats, monitoring of criminal activity, and gathering of intelligence.[12]

According to the *International Journal of Law and Information Technology*, the net effect of this deluge of material is that, "where once LEAs (Law Enforcement Agencies) had to spend incredibly huge amounts of resources in gathering intelligence about those under suspicion, were often through covert operations, but today simple, cheap, and easy technological means exist to monitor everyone and everything. And most importantly our thoughts and actions may now be consumed simply by reading websites and social media networks like Facebook and Twitter."[13]

Social media has emerged as a powerful decentralising force for gathering intelligence—a critical function broadly aimed to swiftly collect and evaluate information fast and accurately for use by policymakers. According to a 2014 research, more than 80 per cent of federal, state, and local law enforcement officers use social media platforms for intelligence on a regular basis.[14] With the growing number of people joining social media platforms globally, this percentage is believed to have risen considerably in 2017.[15] This trend can be attributed, in part, to mounting public demand for faster and more efficient policing following high-profile public crimes that have been widely publicised or recorded on video.[16] The shrinking

12. Nicole A. Softness, "Social Media Intelligence: The Precedent and Future for Regulations", *American Intelligence Journal*, vol. 34, no. 1, 2017, p. 32, at https://www.jstor.org/stable/26497114?read-now=1#page_scan_tab_contents. Accessed on May 2, 2023.
13. Lilian Edwards and Lachlan Urquhart, "Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?", *International Journal of Law and Information Technology*, 24 (3), pp. 279-310, August 10, 2016, at https://academic.oup.com/ijlit/article-abstract/24/3/279/2404493?redirectedFrom=fulltext&login=false. Accessed on May 2, 2023.
14. Alexandra Mateescu, Douglas Brunton, Alex Rosenblat, Desmond Patton, Zachary Gold and Danah Boyd, "Social Media Surveillance and Law Enforcement", *Data & Civil Rights: A New Era of Policing and Justice*, October 27, 2015, pp. 1-2, at https://datasociety.net/wp-content/uploads/2015/10/Social_Media_Surveillance_and_Law_Enforcement.pdf. Accessed on May 2, 2023.
15. Ibid., pp. 1-2.
16. Ibid.

window of reaction time available to the government before being subjected to criticism from blogs and various news outlets has further intensified this pressure. In addition, citizens now have larger access to online influence, allowing them to quickly identify and share their concerns about the failures of the government globally.[17]

BENEFITS OF SOCMINT

It is well acknowledged that content analysis, that is, the study of how frequently words appear in an individual's language, may reveal unique and deeper insights on a person's intent, emotional stability, ways of looking at things, and their viewpoints. Most of the discussions regarding morality and legality of SOCMINT centre on this aspect of the problem, as well as the government's legal right to study certain traits of various segments of domestic and foreign populations. SOCMINT, on the other hand, provides a variety of important advantages to the Intelligence Community. By monitoring the suspects' Facebook profiles, one may learn about their social network position, their impact and influencers, geographical locations, history of content such as their 'likes', and, much more, this intelligence provides useful information. As other methods of analysis, such as network analysis and impact mapping, have become more widely known, the domestic population no longer accepts regulations that are only based on the content of the individual's Facebook postings or tweets.[18]

LIMITATIONS OF SOCMINT

Claiming that SOCMINT has revolutionised intelligence surveillance or that it has reduced the need for auxiliary surveillance by other techniques is premature. While assessing a user's online behaviour and presence has actual advantages, accuracy is not always trustworthy or possible. Observers frequently encounter the problem of *context collapse*, which occurs when statements intended for a limited, cultivated audience are misinterpreted when applied to a wider audience. SOCMINT does not solve these issues of context

17. Softness, n. 12, p. 33. .
18. Ibid.

or nuance. It just broadens the scope of available data collection.[19] Moreover, monitoring this aspect of somebody's life does not allow unrestricted access to their goals or intents. Although no intelligence can give that, there are individuals who might create detailed profiles based on somebody's social media activities. The Department of Homeland Security (DHS) has defined SOCMINT as a "tool for situational awareness, an active knowledge of their surroundings and any risks thereof, made possible such as through monitoring social media feeds regarding various happenings and occurrences in particular geographies."[20]

Terrorist organisations extensively use social networking sites such as Facebook, Twitter, Tumblr, Instagram, Telegram, YouTube, Dailymotion, Blogs, and various other discussion forums such as Reddit to spread propaganda centred on their core radical beliefs and ideologies, target and recruit potential members, and create virtual communities that share a common agenda. Twitter, a popular microblogging platform, is constantly being used as an active platform to disseminate information and communicate during civil unrest planning and execution. For instance, since May 2011, the Taliban has been very active on Twitter, where it had almost 7,000 and more followers; they regularly tweeted through their twitter handle @alemarahweb. Currently this account has been blocked (Twitter page of Taliban, 2019). Tracing the events of the Taliban's takeover of Afghanistan in 2021 reveals that social media played a significant role amidst the chaos. The official spokespersons of the Taliban, Suhail Shaheen and Zabihullah Mujahid, through their official twitter handles @suhailshaheen1 and @Zabehulah-M33, actively promoted and disseminated their propaganda, achievements, on Twitter, as well as portrayed a peaceful transfer of power via their official Twitter handles. However, insider sources and various news reports suggest that the actual reality was far from peaceful.

Another instance of a terrorist organisation using social media for recruiting, according to the South African Banking Risk Information Centre (SABRIC), ISIS is growing its influence in Africa. *The Times* reported that an African version of the Tinder dating app is now

19. Ibid.
20. Mateescu et al., n. 14, p. 6.

being used by ISIS to gather funds for their terror outfit.[21] ISIS operatives use the app by making fake profiles and using pictures of less-known personalities. Single men and women are lured and contacted by ISIS operatives. Intimate conversations, pictures and videos are exchanged, and when the tone of the conversation turns sour and tense, the person is blackmailed and money is demanded. This technique is branded as 'Tinder Terror'.[22] It is important to trace the patterns that ISIS over the years have focused and succeeded in their propaganda game, along with their various techniques of courtship—what we know of as honey trapping.

ROLE OF SOCIAL MEDIA IN GATHERING INTELLIGENCE

The relevance of Open-Source Intelligence (OSINT) and the intelligence that is gathered from publicly available sources have grown in abundance over the recent years, particularly with the prominence of the internet since the early 2000s. Although, OSINT is not restricted to the internet, the medium holds a booming number of data and information. The rise of social media on the internet, in particular, has challenged the use of OSINT. There are various advantages of OSINT, especially on the internet, such as, availability of vast amount of information, cost-effective in nature, and it poses very little risk to the experts of the Intelligence Community, as compared to other disciplines of intelligence collection. Threats to national security can be countered by the Intelligence Community more effectively by investing more significantly in OSINT analysis. With the easy access to OSINT, additional resources may be given to the collection, language translation, and analysis of OSINT internet data for effective use in combating threats.[23]

21. "ISIS funds terror with 'Tinder' love scams", *The Times*, November 14, 2022, at https://www.thetimes.co.uk/article/isis-funds-terror-with-tinder-love-scams-nv08xnbcz#:~:text=At%20face%20value%20it%20looks,once%20the%20conversation%20turns%20sour. Accessed on May 15, 2023.
22. "ISIS funding terrorism with Tinder scams", *The OZ*, November 14, 2022, at https://www.theaustralian.com.au/the-oz/news/isis-funding-terrorism-with-tinder-scams/news-story/ad2cdd9df8005c1a06e6a1f2b561680e. Accessed on May 15, 2023.
23. Sofia Charania, "Social Media's Potential in Intelligence Collection", *American Intelligence Journal*, vol. 33, no. 2, 2016, p. 94, at https://www.jstor.org/stable/26497093?read-now=1#page_scan_tab_contents. Accessed on May 2, 2023.

The benefits of the internet in gathering intelligence, as discussed, increases with the complement of social media, and can also be used to achieve the objectives of counterterrorism. This involves both responding to existing threats by terrorists and predicting futuristic situations that may lead to various terrorist activities.

Sharing Information Is Easier: Social media has now made posting information a lot easier. It serves as a channel through which virtually anybody can easily share any content or information online. The most popular social media platforms are incredibly user-friendly, and are usually free of cost. Posting any content on a web page used to be very time-consuming and required more technical skills, especially with blogging and microblogging, and this was popular before the emergence of social media. Therefore, the use of social media is easier than ever to share various kinds of information, content, etc., with the mass audience.

Due to the easy accessibility of the internet and social media, anybody can post updates, and social media has now become the quickest real-time source of information available.[24] It is true that media broadcasts by the news agencies are exceedingly fast these days, but social media is a step ahead and is unique in nature, as it allows individuals with various unique information to share it directly with the public. During the terrorist attacks in Paris by ISIS, the use of Twitter has clearly proven the speed with which information was shared online through social media; the individuals who witnessed and were taken hostages shared information with the outside world that only they were able to see. For instance, a hostage posted on Facebook, seeking help, stating, "Please come help us! People are being shot one by one! First floor, please quick!"[25]

Terrorist groups cannot regulate what their members do on the internet. Aymen Al-Tamimi, a Middle East Forum fellow who has closely followed the Syrian militant groups, states regarding ISIS that, "it is clear regarding who is managing the official accounts, it is a centralised management, but then there are supporters, and no

24. Omand, n. 9.
25. Brian Patrick Byrne, "Paris Theater Massacre: 118 Killed in Hostage Crisis", *Vocativ*, November 13, 2015, at https://www.vocativ.com/news/250374/theyre-shooting-people-paris-hostages-post-cries-for-help/. Accessed on May 2, 2023.

one has any control over what they do."[26] For instance, in 2014 ISIS instructed all its members to turn off the location services on their mobile phones, so that their movement and whereabouts would not be revealed; however, many members still kept their location enabled on some of their tweets, which revealed the data of their location.[27] According to a study conducted by the Brookings Institution, "a significant number of reports gave valid GPS locations in ISIS territory."[28] ISIS leaders also banned iPhones around the same time due to similar security concerns, but a third of ISIS supporters' tweets were tweeted using iPhones, and little change was observed after the decree, reinforcing the point that, while ISIS may try to control its supporters, it is difficult to regulate what its supporters and members do online.[29] Experts of counterterrorism can potentially take advantage of the little leaked information caused by non-compliant members or supporters on the web, with location data being one of the most helpful sorts of leaks.[30]

Like most social media users, even ISIS members frequently post minor details about their everyday life—an interesting example is a post on snickers bar, "I know I should thank Allah a lot for all the blessings. Never thought I would eat a bar of Snickers here."[31] Counterterrorism and security experts can learn about the everyday lives and views of ISIS members, as well as members of other terrorist organisations who are virtually active by just looking at the content they share casually or frivolously. These experts can also gain a better knowledge of the organisation's functioning structure and opinions

26. Alice Speri, "ISIS Fighters and Their Friends Are Total Social Media Pros", *Vice*, June 18, 2014, at https://www.vice.com/en/article/wjybjy/isis-fighters-and-their-friends-are-total-social-media-pros. Accessed on May 8, 2023.
27. Markham Nolan, "How ISIS' Twitter Army Works", *Vocativ*, March 6, 2015, at https://www.vocativ.com/world/isis-2/isis-twitter-census/. Accessed on May 8, 2023.
28. J. M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter", The Brookings Institution, March 2015, pp. 11-14, at https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf. Accessed on May 8, 2023.
29. Ibid.
30. Charania, n. 23, p. 95.
31. Rukmini Callimachi, "ISIS and the Lonely Young Americans", *The New York Times*, June 27, 2015, at https://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html. Accessed on May 8, 2013.

of the members through such posts, allowing them to effectively counter the activities of terrorist groups.

The following case study is an example of counterterrorism and security experts effectively utilising a "leak" by a non-compliant ISIS member on Twitter, which is a significant platform for spreading propaganda by the terrorist organisation.[32] An ISIS member uploaded a selfie on Twitter boasting about ISIS's *command and control skills*, acting as an example of information irresponsibly made public.[33] Air Force General "Hawk" Carlisle was able to exploit this information to the advantage of the US government, notably the location services related to the post. Following the verification and confirmation of the location, an airstrike was launched, and the ISIS building was destroyed, illustrating how one piece of GPS data was utilised as an actionable information.[34]

Strategy: Analysing terrorist social media strategies can lead to a better understanding of the organisation's on-the-ground operations, so as to better understand how the organisation functions, and build accurate expectations about its future strategies by researching the methods that ISIS uses online and focusing on those that are most successful. Counterterrorism and security experts can identify certain strategies used by ISIS on social media, which presumably extend beyond the virtual realm. For instance, ISIS leverages the concept of empowerment to entice susceptible individuals via social media platforms. Alex's case, a young female convert to Islam, is a prime example.[35] Alex is the kind of at-risk adolescent that terrorist organisations like ISIS target. She is a lonely young woman who battles with "lack of maturity and bad judgement" as a result of foetal alcohol syndrome. Members connect with potential recruits like Alex through social media sites like Facebook, promising the

32. "Hashtag Terror: How ISIS Manipulates Social Media", *ADL*, August 21, 2014, at https://www.adl.org/resources/report/hashtag-terror-how-isis-manipulates-social-media. Accessed on May 8, 2023.
33. Ibid.
34. Michael Hoffman, "US Air Force Targets and Destroys ISIS HQ Building Using Social Media", Military.com, June 3, 2015, at https://www.military.com/defensetech/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media. Accessed on May 8, 2023.
35. Callimachi, n. 31.

benefits of having a purpose in life, fighting for a noble cause, and so on, which is frequently precisely what these disillusioned individuals are looking for.[36]

ISIS carefully and specifically brands its organisation on social media for its diverse audiences. It seeks to look powerful and brutal in the eyes of the West, while it portrays itself as a charitable protector of Islam in the eyes of the people in West Asia. For example, ISIS tweets addressed to the United States are often menacing, such as "You are our targets."[37] Video propaganda targeted at the East, on the other hand, contains footage of members handing over food and emergency supplies.[38] The humanitarian image ISIS aims to project to the Islamic countries (in West Asia and North Africa) through its social media methods can provide experts with insight into how the group garners support in the politically unstable Levant and Africa region in real life. This data can be used by intelligence agencies overseas to strategise and aim to reduce support for such groups.

Social media platforms such as Facebook and Twitter also help the experts of the Intelligence Community to keep a track of how an individual contacts—understanding the terror network. A major challenge for counterterrorism and security experts, according to Daniel Byman, a professor at the Georgetown University School of Foreign Service, and Jeremy Shapiro, a fellow in the Brookings foreign policy programme, is "detecting a terrorist before he acts."[39] They also claimed that Syrian militants' Facebook friends and Twitter followers might be suspected terrorists, and that this information can help analysts determine whom to watch online closely.[40]

36. Alicia Lu, "How Does ISIS Recruit, Exactly?", Bustle.com, September 19, 2014, at https://www.bustle.com/articles/40535-how-does-isis-recruit-exactly-its-techniques-are-ruthless-terrifying-and-efficient. Accessed on May 8, 2023.
37. "Photo implies ISIS threat to Chicago", WGNTV.com, August 21, 2014, at https://wgntv.com/news/wgn-investigates/photo-implies-isis-threat-to-chicago/. Accessed on May 8, 2023.
38. Charania, n. 23, p. 96.
39. Daniel Byman and Jeremy Shapiro, "We shouldn't stop terrorists from tweeting", *The Washington Post*, October 9, 2014, at https://www.washingtonpost.com/opinions/we-shouldnt-stop-terrorists-from-tweeting/2014/10/09/106939b6-4d9f-11e4-8c24-487e92bc997b_story.html. Accessed on May 9, 2023.
40. Ibid.

Recruitment and Expansion: Terrorist groups use social media to recruit new members, disseminate propaganda, and encourage existing members. Experts of counterterrorism can utilise this information to understand more about these groups' larger strategy in order to more effectively fight them. Terrorist rhetoric on social media may be used to understand who their potential targets are. Jihadi websites, for example, portrayed the Bataclan Theatre in Paris as pro-Israel.[41] Though it is not known whether Jihadi social media mirrored this thinking about the Bataclan, counterterrorism experts can watch social media sites to look for similar information that could lead them to other targets. *The Daily Pioneer* has recently published a similar case of ISIS exploiting and identifying the data of potential university targets who exhibit traits and inclinations towards jihad; this data is provided by the Transparent Tribe.[42] Counterterrorism expert, Dr. Rituraj Mate, stated that, "most of the individuals recruited by ISIS possess technical backgrounds and are young in age, creating a dangerous combination for executing terrorist attacks. These individuals, particularly those with engineering qualifications, could be possibly utilised to fabricate sophisticated improvised explosive devices (IEDs) and develop communication applications to evade security agencies. ISIS aims to expand its influence in India by disseminating radical propaganda and targeting vulnerable youths within a specific community."[43] Information such as this may be used to strengthen security in areas where attacks are most likely and counter the strategies of such terrorist organisations.

Modus Operandi: Social media is a source of information that experts of the Intelligence Community may use in conjunction with data-crunching technologies to predict significant attacks. Following the November 13, 2015, attacks in France, analysts at Predata gathered metadata from several online pages and created a model

41. Anshel Pfeffer, "French Intel Predicted Paris Attack, But Got the Timing Wrong", *Haaretz*, November 17, 2015, at https://www.haaretz.com/world-news/2015-11-17/ty-article/.premium/french-intel-got-the-timing-wrong/0000017f-def9-df9c-a17f-fef94d670000. Accessed on May 9, 2023.
42. Rakesh K. Singh, "ISIS recruitment in India sees spike", *The Pioneer*, May 2, 2023, at https://www.dailypioneer.com/2023/india/isis-recruitment-in-india-sees-spike.html. Accessed on May 16, 2023.
43. Ibid.

that effectively predicted the attacks. YouTube, a social networking site, was among the websites from which data was taken. Activities such as page views, number of participants, etc., on terrorist-related web pages was considered by the model, and it revealed a spike in activity on these pages that was above the model's threshold for raising an alert, indicating a high possibility of an attack. This model properly predicted, and retrospectively eight of the previous twelve terrorist events in France.[44] Using information acquired from social media sites such as YouTube, researchers can determine which web pages are seeing unusually high levels of traffic. This may indicate the need for increased vigilance and additional investigation into terrorist activity.

Gauging Public Opinion: Social media enhances the internet's benefits by allowing experts to monitor and evaluate popular sentiment, which assists in the prediction of uprisings. This is important for counterterrorism, as it enables analysts to comprehend and predict political instability, which is one of the factors that may lead to an increase in terrorist activity.[45] Social media is fundamentally a crowd-sourced source of information.[46] Experts of the Intelligence Community can compare the posts of millions of social media users to gain a better understanding of common opinions towards various events and political organisations. With just 11.8 per cent of Twitter users having "protected" or "private" accounts and roughly 50 per cent of Facebook users having "private" accounts, CT experts may read the bulk of posts on prominent social networking sites without infringing any user privacy rights.[47] The posts can be analysed from each social networking site to ascertain the number of individuals who support or oppose specific views, and then generalise from these figures to estimate about larger populations, in a way that the internet would not enable without social media sites.

44. Charania, n. 23, p. 97.
45. Nauro F. Campos and Martin Gassebner, "International Terrorism, Political Instability and the Escalation Effect", IZA.org, March 2009, at https://docs.iza.org/dp4061.pdf. Accessed on May 9, 2023.
46. "Hashtag Terror: How ISIS Manipulates Social Media", ADL.org, August 21, 2014, at https://www.adl.org/resources/report/hashtag-terror-how-isis-manipulates-social-media. Accessed on May 9, 2023.
47. Charania, n. 23, p. 97.

CONCLUSION

Accessibility of the vast amount of information remains a major challenge while using OSINT. It might be beneficial to the Intelligence Community, but, at the same time, it can pose a risk as it aggravates the existing issue of separating signals from noise. OSINT is perhaps the area where one has an abundant source of information and the inference drawn from the existing information remains a complicated task.

A crucial challenge posed by the internet is the difficulty in establishing the veracity of information obtained. It is impossible to restrict the information that individuals can publish on the web globally. Another difficulty with the internet has been the ease with which militant and terrorist organisations get to know the actual situation. Terrorist organisations are more vigilant—"how huge their digital imprint" is, and they exercise caution while engaging in online activities.[48] Going entirely offline is possible for terrorist organisations, although it is very unlikely, as it would limit their ability to recruit and prevent experts from leveraging leaks such as GPS data.

Social media, on the other hand, creates new avenues for terrorist organisations; utilising these platforms to quickly communicate with each other and pose serious threats to government institutions. For example, ISIS uses Telegram, a secure encrypted mobile messaging application—this particular platform offers an option of 'secret chat'. Prior to the event on December 6, 2015, the organisation issued a call for an attack against Saudi and Emirati soldiers in Aden through Telegram.[49] Terrorist group members can also communicate using gaming platforms such as Sony's PlayStation 4. Members can exchange messages or use voice chat in these videogames via the PlayStation Network gaming service. Members may also create messages within the games, such as creating phrases and sentences

48. S. D. Gibson, "Open Source Intelligence (OSINT): A Contemporary Intelligence Lifeline", Cranfield CERES, October 25, 2011, at https://dspace.lib.cranfield.ac.uk/handle/1826/6524. Accessed on May 9, 2023.
49. Colin Neagle, "How ISIS could use video games, messaging apps to evade surveillance", Networkworld.com, November 17, 2015, at https://www.networkworld.com/article/3005364/how-isis-uses-video-games-playstation-4-messaging-apps-to-evade-surveillance.html. Accessed on May 9, 2023.

with bullets on a wall, which other online players can view.[50] Experts of the Intelligence Community struggle to keep track of many systems, and communication techniques like the latter example of creating messages within videogames are practically impossible to trace. Intelligence agencies must invest in developing predictive models that filter through relevant metadata to anticipate attacks before they occur, as well as programmes that can nullify the terrorist organisations' effective use of social media platforms.

Over the years, India too has been at the receiving end of social media terrorism. There have been several events where social media has been used as a tool by the adversaries to wreak havoc. For instance, ISIS has taken advantage of the instability in Afghanistan and asserted itself on Afghan soil. ISKP is using Afghanistan as a launchpad for Jihad and is penetrating into Indian soil. Threats of ISIS have been prevalent, particularly in Kashmir and Kerala. There have been many cases of families, especially from Kasaragod, Kerala, suspected of joining ISIS.[51] This is yet another example of Kerala's Islamic State connection. Over the years, India has witnessed one of the highest surges in recruitment of individuals by ISIS. There are enough evidence and reports that indicate the patterns of ISIS, gathering information of individuals with the help of groups like *Transparent Tribe* to recruit them via social media. Therefore, it is imperative for the state security agencies to keep vigil on social media recruitment channels as intensely as it maintains surveillance over traditional mode of terrorist recruitment. India should enhance its alertness and be more cautious in preventing sensitive information related to its national security from reaching social media. As a nation, India should carefully examine the information received through OSINT and must attempt to enhance its capacity in encryption and cryptography. Data fusion centres should be upgraded to international standards. Lastly, India should enhance its capabilities in developing encrypted applications for an easy flow of information and maintaining its sensitivity.

50. Ibid.
51. "Kerala: Six-member family from Kasaragod on radar of security agencies after they illegally enter war-torn Yemen, suspected of joining ISIS", OpIndia.com, December 25, 2022, at https://www.opindia.com/2022/12/kerala-security-forces-family-six-kasaragod-yemen/. Accessed on May 19, 2023.