ISSN 23939729

CLAWS

No. 137

2026

MANEKSHAW PAPER

Information Threat Detection System (ITDS): An Advanced Software Based on AI & ML Tech for Dominance in Information Operations

Kunal Sharma

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam "Bahadur", was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw's contributions to the Indian Army are legendary. He was a soldier's soldier and a General's General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India's best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.

Field Marshal SHFJ Manekshaw, MC
1914-2008

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

MANEKSHAW PAPER No. 137, 2026

Information Threat Detection System (ITDS): An Advanced Software Based on AI & ML Tech for Dominance in Information Operations

Kunal Sharma

Centre for Land Warfare Studies
New Delhi

Editorial Team : CLAWS

ISSN : 23939729

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone +91-11-25691308 Fax: +91-11-25692347
Email: **landwarfare@gmail.com**, website: **www.claws.co.in**
CLAWS Army No.33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore may not be quoted or cited as representing the views or policy of Government of India, or the Ministry of Defence (MoD), or the Centre for Land Warfare Studies.

Published in Bharat by

Sabre & Quill Publishers, New Delhi, India
www.sabreandquill.com / sabreandquill@gmail.com

Contents

Information Threat Detection System (ITDS): An Advanced Software Based on AI & ML Tech for Dominance in Information Operations

Abstract

The advent of social media and e-media has given a new dimension to the domain of Information Warfare (IW). It has emerged as a tool of psychological operations, propaganda, warfare, and perception management that has faster and wider outreach to directly strike and influence the psychology as well as perception management of any country, selected organisations, and combatants in any conflict zone / environment. It aims to alter behavior that ultimately affects the outcome of any conflict. India as a nation is facing the challenge of insurgency / terrorism as well as continuous threats in the neighbourhood due to border disputes that can escalate to war. However, considering present circumstances, geopolitical aspects, and economics, countries are avoiding any escalation to the conventional threat level and are relying more upon asymmetric or hybrid warfare that remains predominant in the current circumstances without surpassing the conventional threshold. IW has emerged as the low-cost tool of warfare, and both the adversaries of India have garnered expertise in the field of IW, which is evident in the kind of targeted information-related attacks India is facing on social media and

e-media platforms. Operation Sindoor[a] is the latest example that gives insight into how warfare in the future shall unfold in the context of the Indian sub-continent. It involved touching the thin line of conventional warfare by conduct of precision Kinetic strikes using long-range vectors and controlling the information flow while countering the adversary's narratives. The Kinetic damage inflicted on Pakistan during the operation was significant, but at the same time, there is a requirement of understanding & assessing the damage done by disinformation during the conduct of the operation. Hence, there is a need to evolve advanced expertise in Information Operations (IO)[b] by developing a system with integration of Artificial Intelligence (AI) & Machine Learning (ML) tech to – Detect, Destroy & Dominate (3 Ds[c]) the future information threats.

Introduction

At present, it is difficult to identify the increasing information threats with manual intervention and carry out adequate mapping to deny them. The available social media and e-media analytical capabilities can support IO by partially detecting the threats, it doesn't cover the aspects of destruction & establishing dominance over the Information Environment. The IO must have the capability to influence, disrupt, corrupt, or usurp the decision-making of

a Operation Sindoor was the military action conducted by India in the month of May in response to the brutal killings of civilians in Pahlgam, J&K. The operation was textbook demonstration of modern precision strikes aiming for achieving limited objectives and true.

b IO is a comprehensive and comprehensive process of shaping & controlling the information environment across entire peace-conflict spectrum. Propaganda & perception operations are the dimensions of IO that are executed using tools (akin to non-lethal weapons) like social media & e-media in the era of modern warfare.

c 3Ds of Information Operations i.e. Detect, Destroy and Dominate are the capabilities that an IW organisation must possess in modern era of warfare.

adversaries while protecting its own[1]. But the question is in what time frame? During the conduct of military operations, especially in the era of quantum information transmission, speed of the IO capabilities will decide the outcome of dominance. However, the same can be achieved by the use of AI and the deployment of an ML Algorithm.

The research recommends a framework for set of algorithms based on AI & ML for ITDS that will enhance the capabilities in the cognitive dimension of IO by automatically identifying the information threats emerging on social media and e-media platforms to detect, destroy & dominate the source information threats. The threat detection will provide a real-time structured database of various influencers, sources, organisations, and social networks responsible for creating propaganda and narratives impacting military operations. This database will be further analysed by the recommended algorithms to find out the credible intelligence & give out the options to neutralize the Information threats to support their own military operations.

The system will also be suited for understanding the patterns of information attack by adversaries that impact military operations, hence, provide means to develop counter-narratives and even help in sentiment analysis of the population in the civil – military domain in real-time.

Info Threats on Social Media and E – Media Platforms

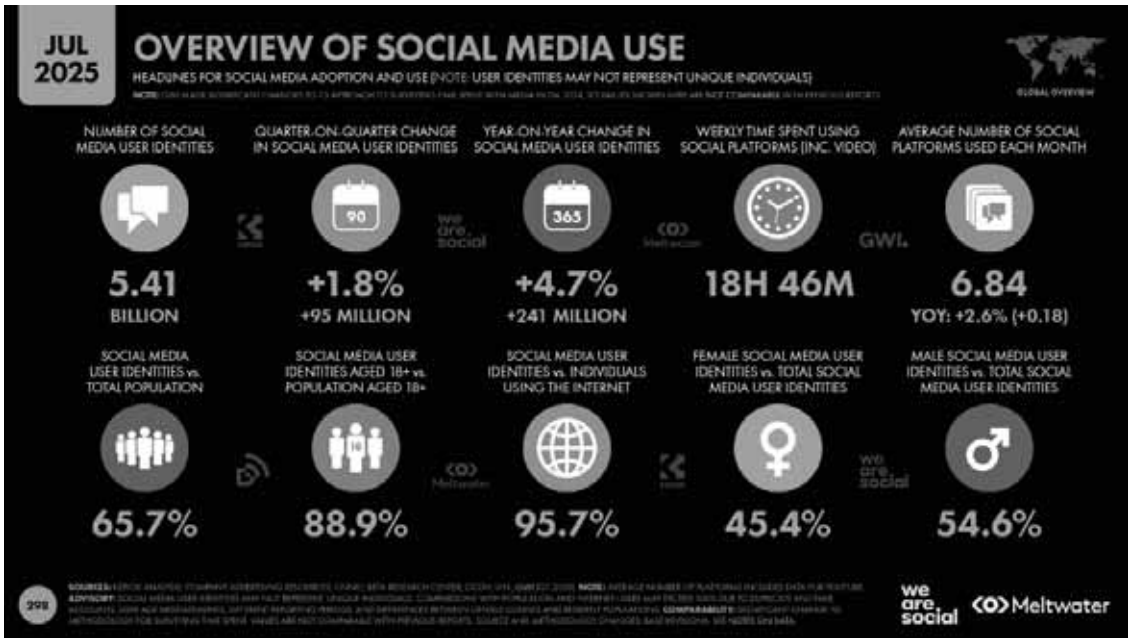


Figure 1. Social Media user base as of Jul 2025, Source Datareportal

Understanding Emerging Threats

The current world population is approximately 8.2 billion, and there are 5.41 billion active social media users, as shown in Figure 1[2]. In the era of modern & hybrid warfare, the info environment plays an important role in shaping the battlefield as the info threats is an ongoing phenomenon that operates beyond the dimension of the battlefield and even timelines of conflict. This part highlights the info threats from a security and military operations perspective.

It has been identified in a study published on Social Media Analysis in Security Journal that *90 % of terrorist activities online are on social media platforms*[3]. These terrorist organisations use social media to propagate their ideology to radicalize masses and hire them. Social media over a period, has emerged as a threat to the nation's security that necessitates the analysis of the same to track info threats. At the same time, it provides an opportunity for the military to use it in its favour in a volatile info environment.[4]

Info threats on e-media platforms are similarly an increasing trend, especially in terms of manipulating facts, biased news dissemination, and increasing fake news sharing on social media platforms. After the Mumbai terrorist attack in 2008, a situation awareness theory analysis was conducted on Twitter now X. It was found that the number of tweets originated from non-government bodies was much higher, which was a sign of panic and uncontrolled sharing of information[5], similar pattern was observed in the Operation Sindoor.

Operation Sindoor had seen the excessive use of social media that was utilized by the Pakistani handlers in spreading fake news and propaganda. See Figure 2[6]. However, the response mechanism adopted to counter the same remained reactive, as it is difficult to assess the impact in the early stages of information spread. As of now, there is limited capability to ascertain such threats manually; such threats generally come to light only after the info environment has been adequately disrupted. The continuous engagement of the media by Pakistan is a well-planned and deliberate

Figure 2. Deliberate misinformation campaign by Pakistan Army during Operation Sindoor.
Source PIB Fact Check X

misinformation campaign to create a global narrative. Such threats can only be countered with proactive threat identification and undertaking countermeasures.

Vulnerabilities of Info Environment

The info threats have evolved tremendously with the advancement in social and e- media especially with the evolution of generative AI platforms like Chat GPT. It has shaped the complete info environment that has challenged the security in both civil and military domains. The quantum data of info, quick sharing and ability to communicate worldwide have introduced new vulnerabilities. These vulnerabilities affect each of the physical, informational, and cognitive dimensions of info environment, see Figure 3.[7]

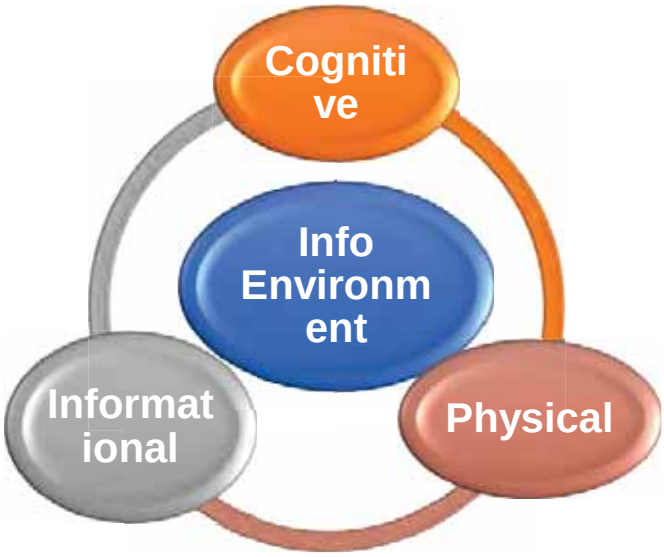


Figure 3. Information Environment

Threats on Social Media

The threats on social media platforms are directly affecting the info environment. Social media is not only vulnerable to attacks by hackers that are limited to hacking systems, DDoS or malware

attacks, but the nature of attacks on social media platforms is information-dominant by terrorists as well as adversary nation-states. In Jan 2010, the Iranian cyber army had hacked into Twitter to use it for distributing malware, and this was discovered in April 2010.[8]

Social media has emerged as a very big source of valuable information that can even be processed to gather military-grade intelligence. Every individual on a social media platform is prone to loss of private information due to continuous data collection. The vulnerability further increases for military personnel who are using social media platforms and erroneously share sensitive information through photographs, revealing their identity. This has even led to an increase in espionage cases, resulting to complete ban of social media platforms for Indian Army personnel.

The info threats that have emerged on social media and are affecting Info Environment in the domain of IO being undertaken by the military are as follows: -

- *Social Engineering:* It is the threat that has emerged due to the availability of personal information on social media platforms. Important persons of state, government officials related to the department of defence, and service personnel, including families, are mainly prone to the info attacks of adversaries. They are prone to sharing info related to place of deployment. Info related to the family can be extracted, and the same can be used against them for espionage. On 23 Oct 2021, one of the Indian Army personnel was arrested in an espionage case, who was honey trapped using Facebook, see Figure 4[9]. The vulnerability of social engineering being exploited by adversaries can be an opportunity to support one's own IO.

Indian Army personnel arrested for allegedly spying for Pakistan's ISI (File photo)

The State Special Operation Cell of the Punjab Police has arrested an Indian Army personnel who was allegedly spying for Pakistan's Inter-Services Intelligence (ISI).

The accused have been identified as Krunal Kumar, a resident of Gujarat posted at Ferozepur Cantt. He was in touch with Pakistani ISI agents while working in the Indian Army's IT Cell.

According to the police probe, Krunal Kumar was befriended by a female Pakistani intelligence officer on Facebook. They soon started conversing over WhatsApp and phone calls. He eventually started passing on sensitive and classified documents to agents across the border through encrypted apps.

Figure 4. News extract of espionage case Oct 2021. Source - ToI

- *Propaganda:* The propaganda threat over social media is pertinent. From corporations using social media marketing to influence the minds of consumers, it has reached to the terrorists using the same for influencing the minds of the public against the state and radicalising youth. In 2016, after the Burhan Wani encounter in South Kashmir, social media was used for mobilising stone pelters and instigating youth. The trend of terrorist / insurgent organisations using social media directly and through their supporters is a norm now. It has become the easiest and cheapest tool of conveying agendas in Kashmir and in any conflict zone / disturb areas.

ISIS has also used social media actively to connect with its global network and inspire thousands with their ideology across the world[10]. However, the same can be exploited by security forces during IO by analysing the sentiment of the public in an area of operation, and further analysis of connections between social media accounts can help in identifying key influencers who can be neutralized. Exploitation of *Geo Tagging*[d] is another aspect that was even used by the US Army during their fight against ISIS, when an ISIS terrorist was tracked using his geo-tagged post, which confirmed his location, after which bombings were conducted to neutralise the target.[11]

- *Fake News* The spread of fake news on social media is another major threat. The speed at which any news is spread makes it difficult to control the damage. The advent of social media has made people citizen journalists who are ready to share anything without any fact-check. The news about the security issues, e.g., Pakistan Social Media handlers shared the fake news of the Rafale shot down by Pakistan Army, see figure 5[12] and in 2019, when India conducted Balakot strikes, social media was flooded with the fake news showing photographs of bodies under debris and rescue operations were shown that were actually old photos of casualties due to earthquake in Pakistan see and figure 6[13].

d Geo Tagging is the process of adding geographic information to any data and same can be accessed through the images, videos or posts that has used the feature of geo tagging activation.

Figure 5. Use of social media for sharing fake news during Op Sindoor 2025. Source PIB Fact Check

Figure 6. Fake photos of Balakot strike trolled over social media - source Times of India

- *Dissemination of Spam and Malware:* Social media can be a source of cyber-attack too. Most of the service personnel who are being tracked can be the targets. There are many links on social media sites that are malicious, but it attracts people to visit. Such links ask for certain permissions that are generally allowed due to a lack of understanding, and the malware enters the system, i.e., smartphones. This may lead to the compromise of sensitive data in the case of a military person; it is like Iran's cyber army hacking of Twitter in 2010. This threat can compromise military operations and the same needs to be considered while operating in an Info environment.

- *Hate Content:* Hate content in an info environment is a silent tool to affect the cognitive aspect of the population by adversaries / terrorists. The info dissemination is such that people continue to follow the hate content without checking of facts. This threat counters the good work being done by security forces in any insurgency-affected area to bring people into the mainstream. There are various groups that are led by certain influencers, and people follow these blindly. The threat needs to be countered through the identification of sources of such content, as well as the spread / impact. This can support one's own IO if exact data is available.

- *Loss of Confidential Information:* This is a major threat, especially for the security forces, that is emerging due to the role of service personnel who are active members of social media platforms. In the context of India, which has implemented a strict social media policy for personnel of the Indian Armed Forces, the cases of espionage due to honey trapping through social media are on the rise. The

other personnel related to DoD[e] also needed to be taken under the umbrella of strict control measures of social media usage to counter the same.

- *Psychological Operations:* The psychological operations being conducted by enemy states using social media can affect the minds of the soldiers operating in any area. After the Indo – China Galwan clashes in the Ladakh region, China continuously released videos of troops mobilisation, exercises, and even photos of soldiers in captivity as part of its informationisation campaign over social media. Figure 7[14] shows a post from a Chinese journalist on a social media platform in the month of November as part of state psychological operation tool. This post was intended to affect the troops' morale in the operational zone. Social media analytics can help in preventing the same by recognising the threat and containing its spread in support of IO. Such URLs can be blocked with timely intervention by the system.

Figure 7. Picture released by Chinese state media of Galwan clashes- source X

e DoD is referred to the Department of Defence where even large number of civilian personnel are working.

Threats on E-Media Platforms

The traditional media platforms like newspapers are losing their space in the new world with the introduction of e-media solutions to include e-newspapers, social media pages, WhatsApp news channels, which is the new trend, in short news where real-time news is updated to keep people engaged, YouTube news broadcasting, and podcasts, including independent journalism, blogs and other digital media formats. Today, people have access to news on their fingertips[15]. The spread of fake news was most prominent during the US elections[16]. This has given a new challenge in the information environment where a large amount of data is already flowing.

The information threat in the spectrum of e-media requiring immediate attention from the security point of view in support of the IO is as follows: -

Fake News: Fake news is news that is intentionally and verifiable false[17]. Fake news is an increasing trend. It is being used by enemy states, terrorists' organisation etc to generate fake content/ information. Such news creates panic and even influences opinion/ minds. It impacts the cognitive aspect in an *Information Environment* that further impacts the decision-making ability of commanders. Detection of such news is essential that circulates in the environment and affect decision making. Figure 8 is showing Fake news that generated controversy during US elections[18].

Figure 8. Image Showing fake news spread during US elections, source - Research Gate

- *Generating Opinion and Debates:* Ability to take decision relies mostly on the type of information we consume; our worldview is shaped based on the information we digest. There is increasing evidence that consumers have reacted absurdly to news that later proved to be fake[19]. This threat from e-media is mainly on the media content shared by news agencies on social media. This generates discussion among the population and may even create divides due to certain opinions.

- *Propaganda:* E-media platform having better outreach than national dailies of any country can be accessed from any part of the world. This gives the advantage for sharing the state-run propaganda news with misleading facts that are difficult to authenticate. This has further affected the domain of IO and needs to be looked after.

- *Morphed Images/Videos:* Images are another content popular on E – Media that can be morphed or manipulated and even related to disconnected news. It is difficult to find the reality of the images until it is adequately analysed. When any such image or video is circulated by any credible e-media source, it is generally considered as correct. It again causes an impact on viewers and further led to generating false opinions. Hence, in an Information environment, it is necessary to detect such images / videos. The impact of this info threat is much faster and affects one's own IO.

This part of the research described varied information threats on social media and e- media platforms that are directly impacting the Information Environment & IO. The same can be countered and even used positively to support one's own IO against the adversary. It has also been understood that the data processed on social media and e-media platforms is quantum, and manual detection of threats is not possible. Only an Autonomous solution can provide a solution for info threat detection that is being covered in subsequent parts.

Understanding Info Related Capabilities to Support IO and Counter Info Threats

Social media and e-media platforms provide big data that can be used for the identification of threats. Analysis of data can provide the capability of early threat detection. In this part, the focus is on understanding the Info Related Capabilities (IRC) that are part of an Info Environment and essential to support IO. The detailed analyses of text of social media posts, geotagged posts by influencers, network analysis on social media, network monitoring to identify attacks, network analysis to identify groups and image identification can mitigate the information threats.

Information Related Capabilities (IRC)

IRCs are the tools and activities that a commander uses to reduce vulnerabilities and to exploit and affect adversaries in the information environment[20]. The IRCs are generally employed to support IO and achieve dominance. The IRCs that are analysed have been taken from the Info Warfare Doctrine of the US DoD. These IRCs are specific to social media and e-media analysis. The IRCs include Intelligence, MISO, OPSEC, MILDEC, Public Affairs, Civil-Military Operations and Key Leader Engagement[21].The various IRC Types are given in subsequent paras with use case in relation to the Info threat mitigation by social media and e-media analysis.

- *Intelligence[f]:* The social media platforms provide a volume and range of information that can be exploited for intelligence collection. Twitter now has X users who update approximately 500 million posts daily[22]. Such posts provide insight into attitudes and behaviours of individuals that is continuously analysed by the algorithms deployed by the social media platforms to personalize the user experiences. This data is further used by various social media analytical companies to better understand their customer base, guiding product development and guiding marketing decisions. Similar analysis can support the IO and help in early threat detection. A geotagged post of ISIL fighter on social media helped the US Air Force to launch a bombing campaign in 2015[23]. Machine Learning and other methods used to process large amounts of data available on social

f Provide population-centric sociocultural intelligence and physical network lay downs, including the information transmitted via those networks.

media platforms can support real-time collection of data on security threats and events.

- *Network Analysis*[g]*:* Information from social media can help in identifying the network or the group that can identify the group's agenda and objectives. Social engineering can help in identifying the insurgents and their network belonging to a particular faction insurgency affected regions by scrutinising the social media profiles of local suspects, and further focusing on the profiles belonging to the insurgents, and their activities could be monitored. This also helps in identifying prominent influencers and closed groups spreading propaganda. Extracting such information is time-consuming and taxing, as manual analyses need to be done that are prone to human error due to limited expertise in the field. Identifying such operatives on social media is difficult but not impossible for those who are engaged in intelligence gathering. However, the application of ML algorithms can support real-time tracking & scrutiny of such a network.

- *Military Information Support Operations (MISO)*[h]*:* The social media and e-media are used extensively for propaganda and psychological operations. Adversaries and terrorists are using these platforms to influence opinions. There is a need to identify sources of such info threats, the spread of such propaganda, and its impact. China employs thousands of people along with AI-enabled machines to post pro-government propaganda posts, messages, and blogs.

g Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments.

h Standardized process designed to meet operational needs by mitigating risks associated with specific vulnerabilities to deny adversaries critical information and observable indicators.

Hezbollah, during the 2006 Lebanon war, edited photos of victims and recovery workers to make the attack genocidal to garner international support, which led the Israel Defence Forces (IDF) to accept a ceasefire, which helped Hezbollah to gain some time.[24] Subsequently, the IDF used a team of citizen reporters to counter this, which provided support that the attack was not against civilians which swayed international opinion. Social media and e-media analysis can help in identifying and understanding the propaganda being used for influencing public opinion, commanders can better anticipate and encourage civil support in the conflict zone, as well as identify possible constraints on the use of force.

- *OPSEC and MILDEC*[i]*:* Cases of espionage on social media and service personnel compromising the sensitive information are continuously on the rise. The threat of deploying malware through social media accounts and gaining access to the computer systems of service personnel and the network is real. Intelligence operatives of adversaries follow personnel related to DoD to find loopholes and gain access to establish connections. It can compromise Operation Security by giving locations of deployment through photos posted by service personnel as well as family members. Social media can spread deceptive information that can be harnessed by malicious actors to encourage violence and incite panic. Few individuals can spread malicious information through thousands of

i Operational Security (OPSEC) is Standardized process designed to meet operational needs by mitigating risks associated with specific vulnerabilities to deny adversaries critical information and observable indicators. Military Deception (MILDEC) are actions executed to deliberately mislead adversary decision makers.

messages. With thorough analysis, OPSEC risk can be identified, and small bits of info gathered can give out larger picture. Although the directives are given to service personnel to control the use of social media, there is a need for an automated system with a human loop to monitor such accounts. Further geotagging is another threat that service personnel don't understand and give away crucial data pertaining to the location, hence, directly raising the OPSEC criticality.

- *Public Affairs[j]:* The public affairs of adversaries and terrorists can be categorized as propaganda & perception control[25]. There is a need to control the same, to control fake / propagated narratives; hence, it is always needed to identify such threats. The traditional media also pick up such info and try to disseminate the same. The security forces' public information department's role is essential here for containing such threats. Again, an automated system can play an important role in countering the same, which should be based on ML algorithms.

- *Civ – Military Operations[k]:* There is a great scope of supporting civil–military operations using social media. Humanitarian aid organizations have embraced social media as a tool to improve their operations. The use of social media is advent during situations of humanitarian crisis. The tools like tweet tracker use Twitter streaming

j Public Affairs are the public information, command information, and public engagement activities directed toward both the internal and external publics with interest in DoD.

k Civil Military Operations to "establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area to achieve US objectives.

Application Programming Interface (API) to retrieve, store, and analyze tweets which are essential during relief operations[26]. Security forces need to monitor such info that impacts the Civ-Mil Operations.

- *Key Leader Engagement*[l]*:* There is a lack of use of social media or media while maintaining OPSEC. The space that military commanders should take for engaging the public has been taken by enemy commanders, terrorist leaders, and influencers who spread their narratives and ideology. There have been many incidents in which the military engages with the public through social media or media as a rebuttal to a particular narrative; however, by that time, the damage has already been extended by deriving a narrative, especially during conflict or in a conflict zone, wherein a lack of connection with the public through social media or media has an impact. Hence, the military leaders at all levels should be able to identify such key leaders of adversaries / leaders with provocative thoughts in their respective Area of Responsibility (AoR)[m] and keep pushing the information as & when required through social media & media based on required time & space. This can be countered by identifying key influencers on social media and media in the AOR of military commanders by using analytics and deployment of specific algorithms focusing the aspect. During the Operation Sindoor, Indian Armed Forces have effectively rebutted the false narrative of Pakistan's military leadership on operational achievements through facts & proofs by

l Key Leaders Engagement can be used to shape and influence foreign leaders at the strategic, operational, and tactical levels to control their opinion spread among followers.

m Area of Responsibility (AoR) is the geographical jurisdiction for a military formation or unit commander.

engaging with public on both social media and media, hence, steering a narrative at not only National but also at the International level that was quite evident through the media reports, even the non-military leaders like ambassador of India to France has appeared on various International media channels to ensure the space not be utilized by adversary leadership in spreading propaganda.

This part of the research has given an understanding of the IRC framework that can be further energized using social media and e-media analytics to counter the information threats.

AI And ML Analytical Methodologies for Developing ITDS

Social media and e-media analytics play major roles in identifying these threats. An automated system based on AI and ML algorithms is a priority requirement that can manage quantum data on social media & e-media platforms to provide real-time monitoring ability. This part of the research covers the various AI and ML-based methodologies/ techniques that can be used for developing a framework of analytical algorithms to develop ITDS for social media and e-media platforms.

Social Media Analytics using AI and ML

There is a requirement to identify the information threat on social media that covers multiple aspects, including scrutinising and classification of big data, structuring of data, and real-time analysis. To achieve the same, there is a need to access the APIs of social media platforms like X and Facebook for data scraping. The datasets need to be identified or created for threats envisaged and accordingly examined using features of posts, such as spatial, temporal, and metadata analysis[27].

The various AI and ML techniques that are applicable for providing social media analytics[28] are described below in Figure 9. These methods are interrelated with each other in formulating an analytics system.

Figure 9. AI and ML based techniques for social media analytics

- *Social Network Analysis (SNA)*: It includes analyses of social media communities and networks by identifying and visualizing social connections of users. The extremist network active on social media can be analysed by identifying seed accounts of extremists known as stars, and their followers can be identified by analysing directionality to ascertain any connection. It is difficult to identify the network manually; however, initially, seed accounts that are generating threats using social engineering. A clustering ML Algorithm will help in finding the common accounts with similar ideology and connections. The steps being followed are given in figure 10.

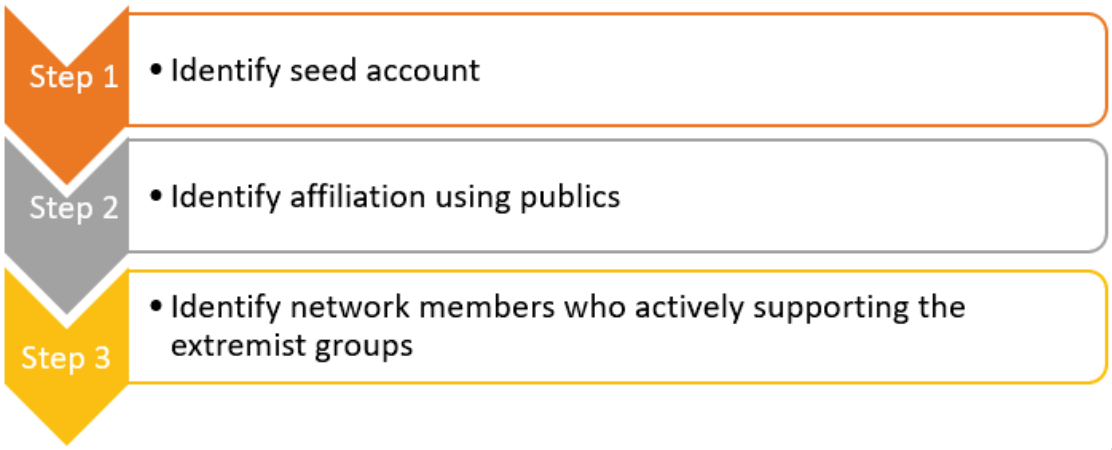


Figure 10. Steps of SNA

- *Publics:* Publics are a unit of analysis in public persuasion, people sharing a common language to address common aspects. This type of analysis focuses on the set of people who care about an issue and use shared discourse to affect debate. It helps in community detection and identifying common groups on social media. This can help in further sorting out the micro communities that are propagating a common ideology in the info environment. An analysis was carried out based on the ISIL network by RAND[n] on X data from July 2014 to May 2015, which helped in drawing Pro and Anti ISIL Metacommunities[o] on X see figure 11[29]. It uses a classifier algorithm along with NLP.

n RAND corporation is an US based Non-Profit research organization that develops solutions to public and policy challenges.

o Metacommunities are the major networks which are distributed in a region connected with same agenda, however, they have different approach.

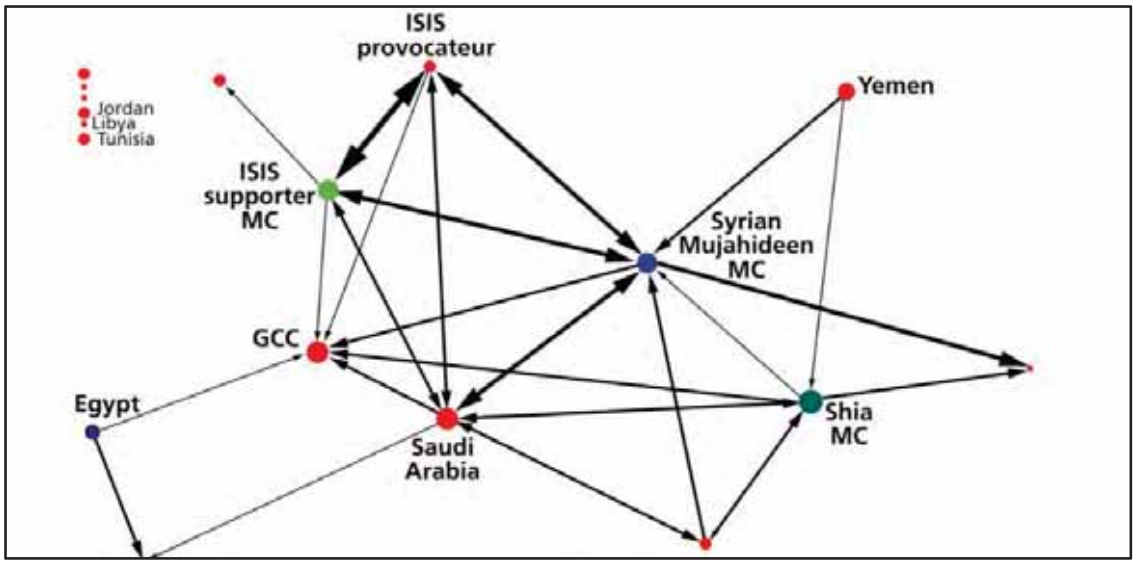


Figure 11. Pro and Anti ISIL Network is identified using SNA and Publics. Source RAND

- *Lexical Analysis*: Lexical Analysis uses statistical tests to count word frequencies, word distance, and other features of the data to detect patterns and data structure to identify common members with similar views. It is an important aspect to identify the word frequency. Semantic analysis, part of NLP, is also used for the same once tokenisation is complete[p] and lemmatisation[q] of words is carried out.

- *Stance* and *Sentiment Analysis*: It helps in identifying the propaganda, hate content, and psychological operations-related threats over social media platforms. It identifies the negative, positive, and neutral stances of words using NLP and Naïve Bayes algorithms[r].

- *Geo Location* and *Geoinferencing*: The social media messages posted are having geographical data in it. Geo location used

p Tokenization process of NLP for breaking words

q Lemmatization process of NLP for removing punctuations

r A type of Classification algorithm

geo stamping and is highly accurate. In an info environment, it can be used to identify the locations of the members who are responsible for producing hate content and validating their profile data. The same needs to be checked for the service personnel who may compromise the OPSEC. Metadata[s] It is used to make inferences about the locations.

- *Deep Neural Networks* (DNN): DNNs are part of Deep Learning (DL), a branch of AI as shown in Figure 12. Social media has voluminous data to share that is ranging from text, photos, and videos. As per an article in Clover DX, study done by Statistia has given some facts about the data of social media produced in 2020[30] see table 1. This data is so huge in Zettabytes that it is not humanly possible to study, hence, machine intervention is necessary. The images and videos are the major source of communication by extremists and enemy states for producing info threats. These threats can be identified using the techniques of DL to identify images and videos that can analyse the features in fraction of time. For example, in insurgency-infected areas, there are photographs circulated showing the atrocities of security forces. These photos are morphed and shown in the wrong context. Such info threats can be detected using CNN and DNN[t] techniques that analyse the data in detail to identify its correctness; moreover, when

s Meta data means data about data e.g Metadata for a document include details of author, file size, data related to document creation, key words to describe document, URL details where data was published. Very useful for analytics and can give out crucial information related to data.

t CNN and DNN are the branches of Artificial Neural Network in which machines are trained to identify images and videos using artificial neurons similar to human brains. Small filters are employed to analyse images in detail.

deployed with other analytical tools like Metadata identification, it gives out details of info source that can support IO in mitigating the origin of the threat.

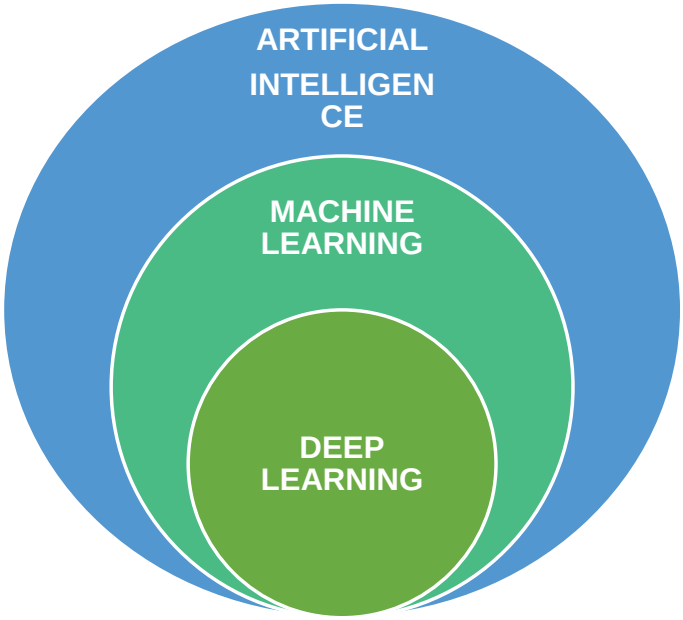


Figure 12. Relationship between AI, ML and DL

1.7MB of data was created every second by every person.
Every day 306.4 billion emails are sent
In 2019-20, 90 percent of the world's data has been created
350 million photos are uploaded to Facebook every day.

Table 1. Facts regarding data on social media, source CloverDX

Outcome 1: The various methodologies/techniques that are being used for social media analytics are not applicable in isolation, but rather in combination with the various approaches as discussed. A *Composite Framework for Analytics Tool* is recommended based on the methodologies that apply varied AI, ML, and DL techniques. For example, Lexical Analysis and publics is used together to form a linguistic model that uses language to identify key words of extremists, identify the frequency of words

to deduce the groups' influencing capability which can be ranked accordingly.

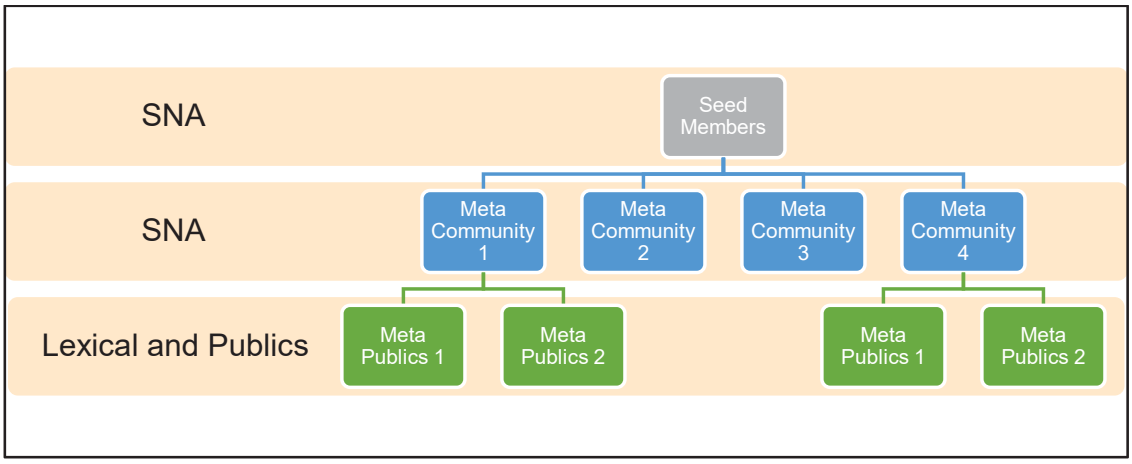


Figure 13. Composite framework showing Social Media Analytics working for identification of communities and closed groups using various methodologies/techniques

Figure 13 shows how the composite framework will be designed to make an analytical tool. SNA is used for identifying the metacommunities, and further Lexical and Publics is used for identifying metapublics[u]. A critical takeaway is that while a team of analyst reading millions of tweets, a single analyst using lexical analysis to identify hundreds of words to characterise them as a close community as public[31].

E-Media Analytics using AI and ML

The major threats to e-media platforms are Fake news, propaganda, generating debates, and sharing of morphed images / videos. These threats were discussed in detail in the previous part. Identification of Fake news is a challenge, as globally, the quantum of data is generated by news sources. The machine-based analysis

u Metapublics are the closely associated communities with same agendas, Meta communities are divided as per regions or some other factor or feature or trait.

approach requires techniques of NLP as the data is text-heavy with different languages.

- Research conducted in the field considers the understanding of features of news to apply analytical techniques. The features are described as under that consider news content and news source for identification of fake news content[32].
    - *News Content*: It comprises a headline, text, images, and videos for which image processing techniques as well as text analysis techniques are applied. The main features need to be identified for processing are as follows: -
        - *Language Structures (SYNT)*: It is a technique of implementing sentence-level features to include word count per sentence. The quality of writing is identified to include world categories like nouns, verbs, pronouns, and adjectives. This evaluates the writer's style and text quality.
        - *Lexical Features*: To identify the number of repeated words and judge the grouping to identify the scope of the text.
        - *Psycholinguistic Cues:* Linguistic Enquiry and Word Count (LIWC) is used for extracting features to identify persuasiveness and biased language. LIWC uses a comprehensive dictionary to categorise words into various psychological, social, and linguistic categories, such as positive or negative emotions, cognitive processes, and social processes.
        - *Semantic Structures:* Semantic structures organize and relate data or concepts to map out meaning in language. The toxicity of a text can be analysed

using the semantic features of the news articles. This enables machines to extract intended meanings, emotions, and nuances in text, facilitating applications like sentiment analysis.

- *Subjectivity Cues*: These are the linguistic indicators within text or speech that reveal a speaker's or writer's personal opinions, attitudes, emotions, beliefs, or interpretations rather than objective facts. Using Text Blob's API[33] for computing subjectivity and sentiment scores of a text can be extracted.

- *News Source*: This is an important aspect for identifying the credibility of news. The news source is just like metadata that provides details of features like URLs, location of the source, domain credibility, trustworthiness, etc. There is a need to create a data set of all the credible media sources to identify their correctness once the machine is trained on the datasets and deployed for analytics.

Outcome 2: **E-Media analysis** is like the social media analysis that requires a framework of multiple techniques integrated into an algorithm. The research carried out in this domain has suggested the use of ensemble methods[v] [34]. The suggested algorithm is based on the techniques of NLP as quantum text data is involved for scraping and analysis, along with CNN for image classification and other ML algorithms. The suggested model for the analysis of news articles is given in Figure 14.

v Ensemble Method is a technique in which multiple algorithms are used for better analysis and result.

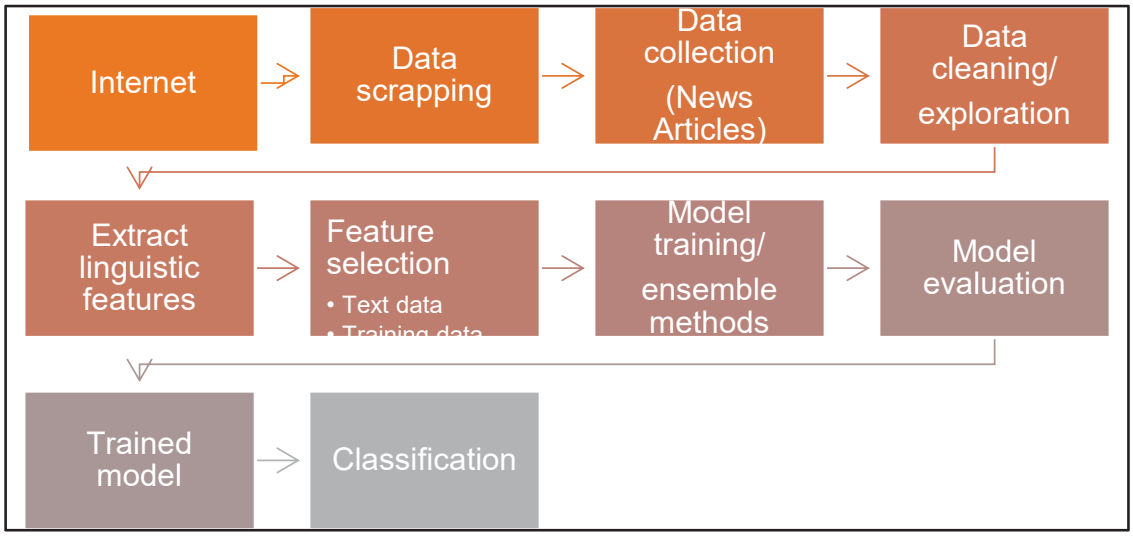


Figure 14. Workflow of training algorithm and classification for news analysis to identify fake news

The social media and e-media analytics can support identifying the threats online and even counter it that can help in achieving dominance in IO. The system as considered while understanding the scope of the research, is possible to be developed.

Proposed ITDS Framework based on Outcome 1 & 2

The research in previous paras has covered various info threats in the information domain that affect the military operations directly or indirectly. Various methods based on AI, ML and DL were covered to understand how analysis can be done to mitigate the threats. The methods covered has already been tested in parts against ISIL to identify its worldwide network and in support of military operations to neutralize identified threats. Hence, the recommended algorithms based on Outcome 1 and Outcome 2 can be a game-changer in the field of IO.

This part focuses on the proposed ITDS Framework based on AI & ML algorithms. However, certain legal & ethical challenges need to be addressed and understood as the proposed technology

shall have access to the private information of users on social media platforms, raising privacy concerns.

Considerations/ Challenges for the ITDS

- *Legal Stature:* The IW domain directly deals with the information of public as well as private nature that entails no boundaries. Social media started from simple social interactions have reached a level of privacy breach as it holds & controls the personal data of users. It has been used as a domain of ideological movement and intelligence gathering that has raised concerns among the public as well as states. The data collection by social media companies is being used as source of revenue by selling it to third parties in the name of understanding consumer behaviour or product improvement. However, data collection or monitoring of social media for corporate and national interest are two separate aspects. In India, there is a need to introduce a law to support the monitoring of social media to make ITDS a legitimate system. Monitoring foreign and own citizens' data for national security matters should be considered as legal and become part of the law.

- *Ethical Issues:* Ethics entails monitoring of data without any bias. The authority given for such a task should not have any contradictory approach for monitoring the social media accounts.

- *Doctrine:* The technology for supporting IO is necessary to be incorporated as part of the IW doctrine. Various aspects, from monitoring to actions to be taken for mitigation of threats, need to be evolved for active IOs.

- *Enterprise System Vs Outsourcing*: The system involves complex technology; however, there are companies like Meltwater[w] that are already working in the field of social media and media monitoring see figure 15. Node XL is another program that clusters and synthesizes social network data; it can mine Facebook likes pages without a password[35]. Hence, a call needs to be taken on whether the ITDS be outsourced or developed as an enterprise solution, considering the aspect of national security.

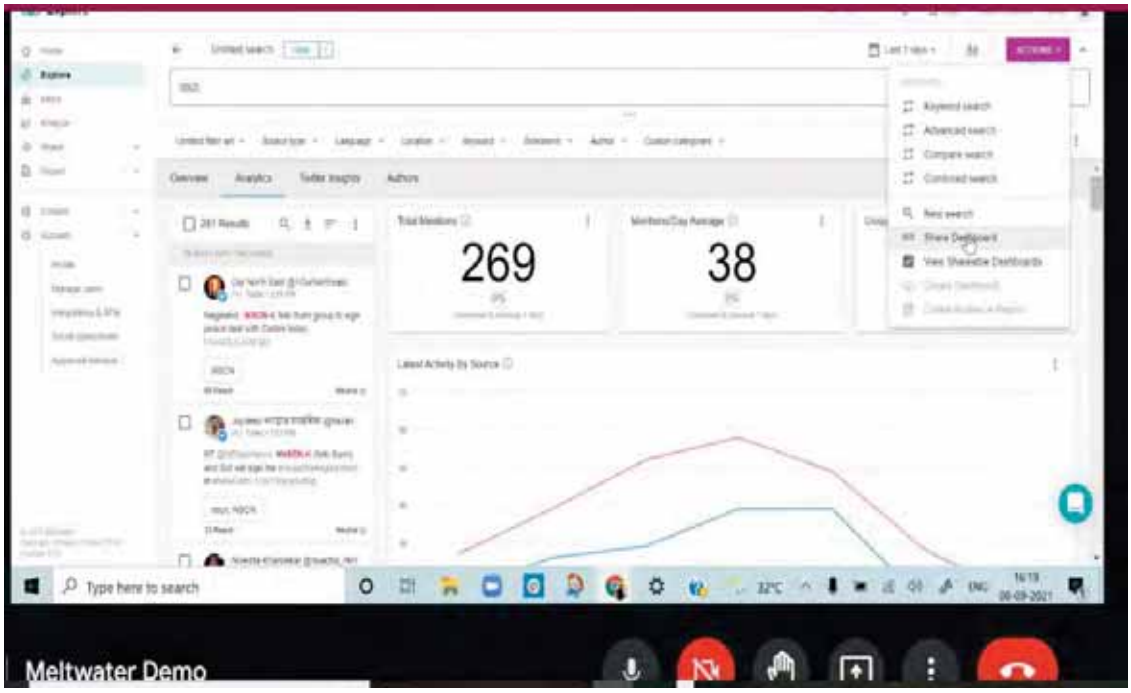


Figure 15. Meltwater media analytics software demonstration taken to understand the capability

- *Centralised Vs Decentralised System:* AI based system generally work effectively with the big data as the ML model is trained efficiently and more accurately. However, the ITDS system will be detecting threats to support IO that

w Meltwater is social media analytics company which is working for corporate and providing solutions for monitoring consumer behaviour. The company has given demonstration of their work to support our research work. It has access to the API of twitter for analytics.

is based on the specific theatre of operations. Hence, there is a need to train the model centrally and the system be deployed as a decentralised model at strategic, operational, and tactical levels with a central repository. The emerging threats in any theatre can be identified in real time and can be mitigated.

ITDS Framework

ITDS framework shall incorporate data collection, data structuring, data classification, data analysis, and decision-making. See Figure 16 [36], The data collection from social media sites like Facebook and X entails data scraping through API calling. There can be reservations among these private entities in giving access to the government; however, these permissions are a prerequisite for the data scraping, and the same should be covered by the legal and ethical code of conduct to make a robust and advanced system under the umbrella of National Security measures.

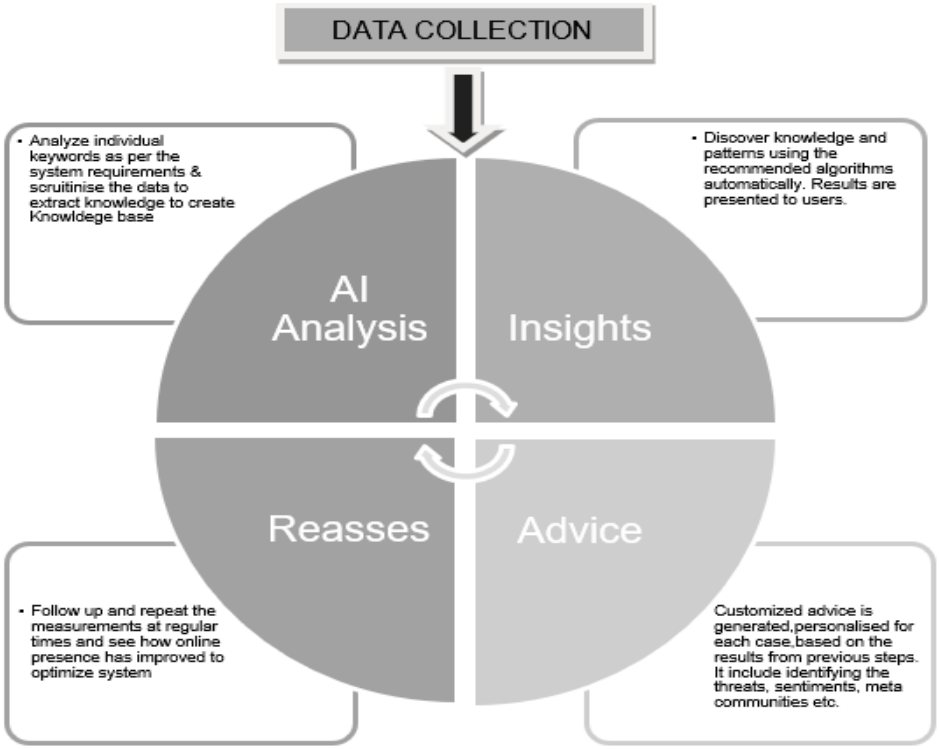


Figure 16. Process of Analytics

Proposed Social Media Analytics Model

The proposed system will analyze the social media posts in real time. The steps need to be followed are elaborated in subsequent paras refer to Figure 17.

- *API Access*: The API rights of social media sites require monitoring need to be obtained.
- *Data Gathering*: The unstructured data will be collected using various methods, such as data scraping, based on relevant parameters[37].
- *Classification*: The data extracted will be classified in groups and techniques like SNA, Lexical, and Publics to find groupings. In this even KNN classifier can be used. CNN will be used for clustering images and videos.
- *Generating Inferences*: The data will be analyzed to generate the following inferences to support IO and mitigate info threats.
    - Identifying seed accounts.
    - Identification of suspected groups and pages.
    - Scrutinize likely bots and fake profiles.
    - Conduct of Sentiment Analysis.
    - Geo-location and geo-inferencing of threat sources.
    - Identifying Key Influencers and tracking them.
    - Identification and monitoring of service personnel.
    - Scrutinizing fake content affecting security environment.

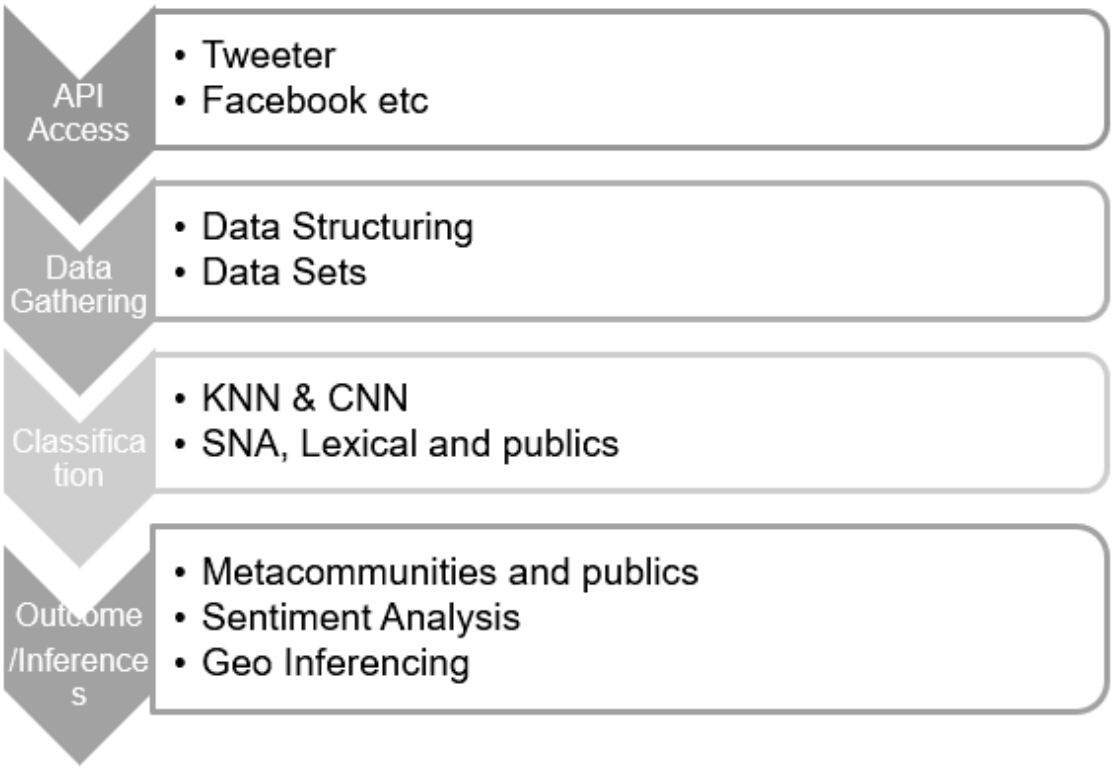


Figure 17. Proposed Social Media Analytics Model

Proposed E-Media Analysis Model

The model will be based on the NLP techniques that will be using ensemble methods while applying ML Algorithms for the detection of info threats based on E – Media platforms. It will be scrutinising the content and source that can help in the identification of the threat.

- *Data Gathering*: There is a quantum of e-media sources. There is a need to create a database of important news sources, including regional media platforms. The data should be scrutinised as per metadata to formulate a dataset that includes the following:
    - Name of news platform.
    - Credibility.

- Writers and contributors.
- Type of media.
- URL details.
- Geo location.
- Language uses.
- Ideology or Agenda if any.

- *Data Classification*: The data is classified based on the content, as per various features as covered in the e-media analytics, to drive Outcome 2.
- *NLP Process:* The data, once classified further the language analysis is conducted to break down the sentences, and semantic analysis is carried out to identify the stance of the documents.
- *Ensemble Methods*: Ensemble method is used for analysis, multiple algorithms like random forest, voting classifier (RF, LR, KNN), bagging classifier (decision tree), and boosting classifier are applied for results[38].

Training of Algorithms and Datasets

Datasets concerning Fake news detection are already available on data repositories like Kaggle that can be used to train machines, initially see figure 18[39]. However, there is need to create datasets that apply to the requirement for information threat detection. It should be elaborate and should include key data commonly used by adversaries and extremists. This can support the initial optimisation of the system.

Figure 18. Fake news detection using Kaggle dataset, source Kaggle

Recommended Software Architecture of ITDS

The framework, as discussed, has paved the way to develop a software architecture for the ITDS for the mitigation of info threats. The recommended architecture based on the research will give the final pathway for developing the two submodules of the software, i.e., "*Social Media Analytical Module*" and "*E-Media Analytical Module*" for achieving *Total Information Dominance*[x]. See figures 19 and 20, respectively.

x Total Information Dominance can be referred to a scenario during a military conflict wherein enemy is isolated in the Info environment and all means of info disseminations has been rendered ineffective ensuring total control of the narrative.

Software Architecture: Social Media Analytics Module

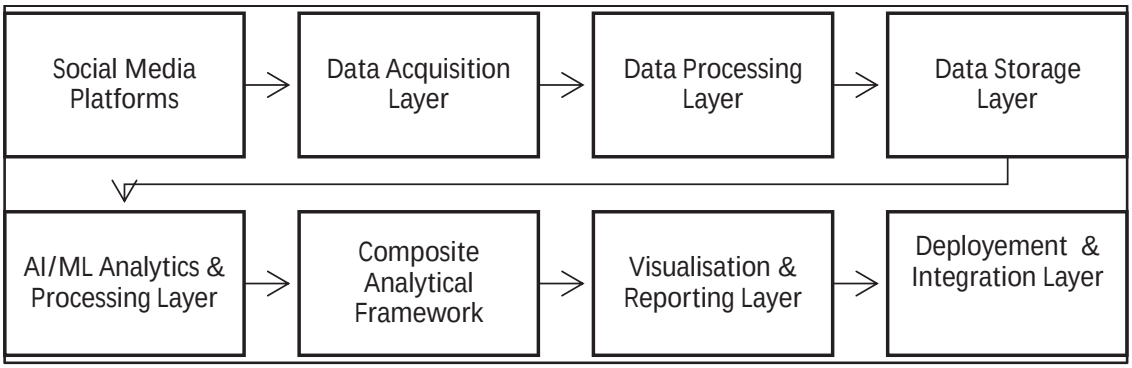


Figure 19. Diagram representing the Software Architecture of the Social Media Analytics Module.

Software Architecture: E-Media Analytics Module

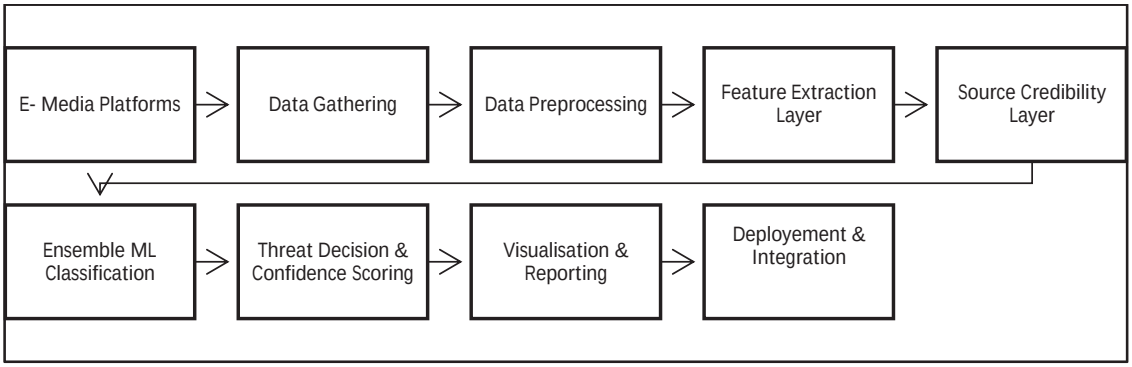


Figure 20. Diagram representing the Software Architecture of the E-Media Analytics Module.

Conclusion

The research aims to develop an AI and ML-driven software designed to mitigate information threats across social media and electronic media platforms. The proposed software, referred to as ITDS, will autonomously detect and respond to such threats to establish *Total Information Dominance*. Once trained on diverse datasets featuring real-time threat patterns, it will monitor these platforms continuously and effectively. ITDS can support military operations in insurgency-affected regions and counter adversarial information campaigns or propaganda. The system will be

deployed according to theatre-specific requirements and integrated with a centralized repository. In modern warfare, IW has become an indispensable component, and ITDS offers a strategic, operational & tactical advantage by enabling superior information control. Beyond threat detection, it will generate actionable intelligence to assist kinetic operations and provide sentiment-based predictions to enhance decision-making during military missions.

References

1 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, "Monitoring Social Media," RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1742.html (Accessed on 08 September 2021 & 25 June 2025).

2 Global Social Media Statistics, Kepios, Datareportal, https://datareportal.com/social-media-users. (Accessed on 28 Sep 2025).

3 R. Medina, "Social Network Analysis: A case study of the Islamist terrorist network," Security Journal, vol. 27, no. 1, pp. 97-121, 2014. https://www.researchgate.net/publication/255718308_Social_Network_Analysis_A_case_study_of_the_Islamist_terrorist_network. (Accessed on 21 October 2021, 25 June 2025 & 08 October 2025).

4 Pooja N Jain and Archana S Vaidya, "Analysis of Social Media Based on Terrorism - A Review," Vietnam Journal of Computer Science, vol. 8 No.1, pp. 1-21, 2021. https://www.researchgate.net/publication/341594046_Analysis_of_Social_Media_Based_on_Terrorism_-_A_Review#:~:text=Analysis%20of%20Social%20Media%20Based%20on%20Terrorism%20%7C%20A%20Review,how%20to%20detect%20acts%20of. (Accessed on 11 November 2021 & 05 September 2025).

5 Ibid.

6 PIB Fact Check. [@PIBfactcheck]. (2025,May 07)Social media posts falsely claims that Pakistan destroyed Indian Brigade Headquarters. [Tweet] X Twitter https://x.com/pibfactcheck/status/1919922375069409298?s=46 (Accessed on 26 February 2025)

7 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1.

8 Dr. Alpana Upadhyay, Dr. Priyanka Sharma, Hardik Gohel, "Analysis of Social Media Attacks and Classify Advances to Preserve," International Research Journal of Engineering and Technology, vol. 2, no. 3, pp. 708 - 711, 2015.
https://www.irjet.net/archives/V2/i3/Irjet-v2i391.pdf. (Accessed on 15 November 2021, 12 August 2025 & 05 October 2025).

9 Yudhvir Rana, Army jawan held for sharing classified info with Pak's ISI, Times of India, 23 Oct 2021
https://timesofindia.indiatimes.com/india/army-jawan-held-for-sharing-classified-info-with-paks-isi/articleshow/87229369.cms#:~:text=This%20story%20is%20from%20October,money%2C%20according%20to%20the%20release. (Accessed on 12 November 2021, 20 July 2025 & 05 October 2025).

10 R.Media, no.2.

11 William, Meagan, Christopher, Lauren, no. 1.

12 PIB Fact Check. [@PIBfactcheck]. (2025,May 07)Beware of old images shared by pro-Pakistan handles in the present context! An #old image showing a crashed aircraft is being circulated with the claim that Pakistan recently shot down an Indian Rafale jet near Bahawalpur during the ongoing #OperationSindoor. [Tweet] X.
https://x.com/pibfactcheck/status/1920025620655874361?s=46 (Accessed on 26 February 2026).

13 Times fact check, "Images of destruction caused by earthquake in Balakot shared as IAF air strike impact", 28 February 2019,
https://timesofindia.indiatimes.com/times-fact-check/news/images-of-destruction-caused-by-earthquake-in-balakot-shared-as-iaf-air-strike-impact/articleshow/68194890.cms. (Accessed on 14 November 2021 & 10 October 2025).

14 Shen Shiwei, Twitter (now X) post, Nov 7, 2021, 08:06 A.M.
https://x.com/shen_shiwei/status/1446734079529914372. (Accessed on 14 November 2021)

15 Iftikhar Ahmad, Muhammad Yousaf, Suhail Yousaf and Muhammad Ovais Ahmad, "Fake News detection using machine learning ensemble methods," Wiley online Library, Complexity,17 October 2020,
https://www.researchgate.net/publication/346262009_Fake_News_Detection_Using_Machine_Learning_Ensemble_Methods. (Accessed on 15 November 2021 & 05 October 2025)

16 A. D. Holan, "Lie of the year : Fake news," *Politifact*, 13 Dec 2016. https://www.politifact.com/article/2016/dec/13/2016-lie-year-fake-news/.

17 Julio C.S. Reis, Andre Correria, Fabricio Murai, Andriano Veloso, Febricio Benevenuto, , "Explainable Machine Learning for fake news Detection," in WebSci '19: Proceedings of the 10th ACM Conference on Web Science, Boston, Massachusetts, USA, 26 June 2019. https://homepages.dcc.ufmg.br/~fabricio/download/websci-reis-2019.pdf. (Accessed on 10 December 2021 & 10 October 2025)

18 Amey Uday Parulkar, Identification of fake news using blockchain, University of West London, 30 November 2021, https://www.researchgate.net/publication/362644804_Amey_Dissertaion_Identification_of_fake_news_using_blockchain. (Accessed on 10 December 2021 & 10 October 2025)

19 J.Soll, "The long and brutal history of fake news," Polotico Magazine, vol. 18, 18 December 2016. https://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535/.(Accessed on 20 July 2025)

20 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1, p10.

21 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1, p11.

22 David sayce, how many posts are published on X in 2025, https://www.dsayce.com/digital-marketing/tweets-day/. (Accessed on 08 October 2025)

23 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1, p11.

24 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1, p16.

25 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1, p22.

26 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1, p23.

27 Pooja N Jain and Archana S Vaidya, no. 5.

28 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no. 1.p28.

29 Elizabeth Bodine-Baron, Todd C. Helmus, Madeline Magnuson, Zev Winkelman, “Examining ISIS support and opposition networks on twitter”,RAND Corporation, 2016, p23. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1328/RAND_RR1328.pdf. (Accessed on 15 November 2021 & 10 October 2025)

30 "Cloverdx," Cloverdx, 23 April 2021. [Online]. Available: https://www.cloverdx.com/blog/how-much-data-will-the-world-produce-in-2021. (Accessed 2 Nov 2021). (Accessed on 15 November 2021)

31 William Marcellino, Meagan L. Smith, Christopher Paul, Lauren Skrabala, no.1, p

32 Iftikhar Ahmad, Muhammad Yousaf, Suhail Yousaf and Muhammad Ovais Ahmad, no 15

33 T. blob. [Online]. Available: www.textblob.readthedocs.io/en/dev

34 Iftikhar Ahmad, Muhammad Yousaf, Suhail Yousaf and Muhammad Ovais Ahmad, no 15.

35 Pooja N Jain and Archana S Vaidya, no 5.

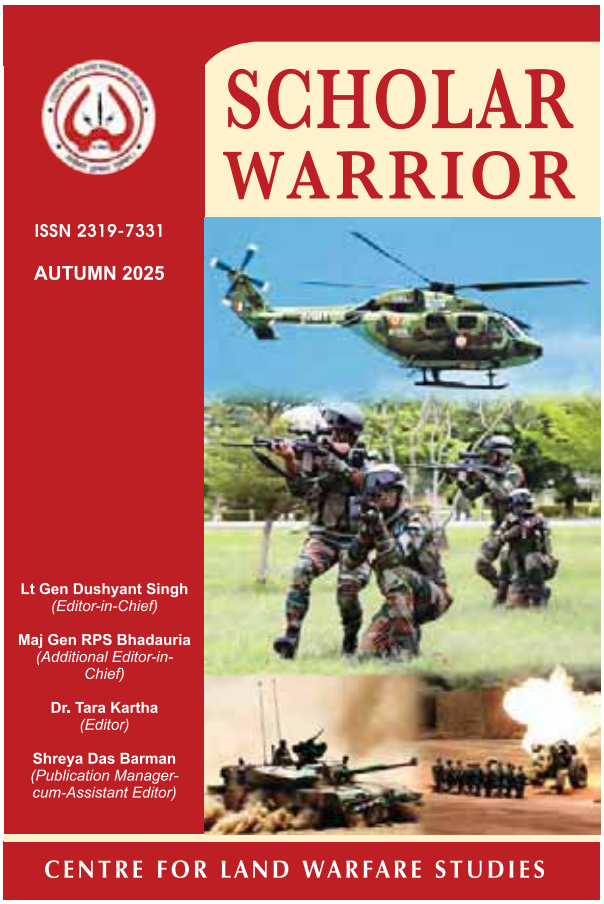
36 Emmanouli Perakakis,George Mastorakis, Ioannis Kopanakis, "Social Media Monitoring: An innovative intelligent approach," Design, pp. 1-12, 20 May 2019. https://www.mdpi.com/2411-9660/3/2/24 (Accessed 14 November 2021)

37 Pooja N Jain and Archana S Vaidya, no. 5.

38 Iftikhar Ahmad, Muhammad Yousaf, Suhail Yousaf and Muhammad Ovais Ahmad, no 15.

39 Kaggle, "Kaggle," Kaggle, 2021. [Online]. Available: www.kaggle.com. (Accessed on 05 November 2021)

SUBSCRIBE NOW



SUBSCRIPTION RATES

IN INDIA
☐ Rs.500/- per copy

SAARC COUNTRIES
☐ US $ 15 per copy

OTHER COUNTRIES
☐ US $ 20 per copy

☐ Rs.1000/- Annual Subscription (2 issues)

TO SUBSCRIBE SEND YOUR REQUEST TO

Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi - 110010
Tel: +91-11-25691308
• Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com
www.claws.co.in

India faces challenges from insurgency, terrorism, and border disputes with its western and northern adversaries that could escalate to war. However, given current circumstances, geopolitical factors, and economic considerations, countries are avoiding conventional escalation, instead relying on asymmetric or hybrid warfare. IW has become a low-cost warfare tool, and India's adversaries have developed expertise in this area, as evident from targeted information attacks on social media and e-media platforms. This has added a new dimension to Information Warfare (IW), it has emerged as a tool for psychological operations, propaganda warfare, and perception management, with a faster and wider reach to directly influence the psychology and perception of countries, organizations, and combatants in conflict zones.

Operation Sindoor highlights how future warfare may unfold in the Indian subcontinent, involving precision kinetic strikes and information flow control. While kinetic damage was significant, assessing disinformation damage is crucial. To counter this, India needs advanced Information Operations expertise, integrating AI and ML technologies to detect, destroy, and dominate (3Ds) future information threats to achieve 'Total Information Dominance'. Information Threat Detection System is such a conceptual software system if implemented, that can be the game changer in the field of Information operations.

• • •

Lieutenant Colonel Kunal Sharma has been commissioned into the Infantry and has been serving in the Army for the last 15 years. He is an alumnus of the Indian Military Academy, Dehradun, and attended various military courses, including the prestigious Defence Services Technical Staff Course at Military Institute of Technology, Pune. During his career, he has held various command and staff appointments at unit, formation, and Army HQ level. He has varied experience of serving in Highly Active Field Areas along the Northern and Western borders, Counter Insurgency operations in North East, and UN Peacekeeping Mission in South Sudan.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributors aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Website: www.claws.co.in Contact us: landwarfare@gmail.com

SABRE & QUILL

MRP: ₹ 100.00 US$ 5.00