Open-Source Intelligence (Osint) For National Security: A Counter Terrorism Approach In Pakistan

*Lt Cdr Tanveer Rafique**

ABSTRACT

OSINT is intelligence gathered from publicly available information. The significance of OSINT takes up due to frequent internet usage. Worldwide connectivity through social media has also revealed unprecedented challenges to existing intelligence organizations/ LEAs. In this context, developed countries established dedicated OSINT centers. However, debates on its reliability and efficacy are still persistent. Research analyzes the efficacy of OSINT to meet national security requirements. It is qualitative with an action research approach tapping into analyse the quality of data. The essential rationale of OSINT for national security with a perspective of counter-terrorism is the product of this study. OSINT application is validated on 4P CONTEST - counter-terrorism model of UK. Opportunities for Pakistan have been highlighted considering the advantages and disadvantages of OSINT tools and methods. Research revealed that, globally OSINT is a new term and lacks an agreed-upon definition. However, the field is highly understudied in Pakistan; there is no local literature available. The paper concludes by highlighting a need for dedicated OSINT organizations.

Keywords: *National Security, Counter Terrorism, OSINT, Data Mining*

* The author is a graduate of Pakistan Navy War Collage 51st Pakistan Navy Staff Course

INTRODUCTION

Humans are born in fear for their survival. Formulation of communal groups for survival may be seen as foundation of the nation formulation process. Perceived security is always higher than apparent security which results in insecurity and inferiority; thus, generating a continuous struggle for security. The expression of national security comprises the term "nation" and "security". If security means a state of being free from danger; national security is simply a nation free from threats. However, freedom from threats is not achievable in practice. Accordingly, national security may be regarded as "a nation in control of its threats."[1] The control over threats is not achievable without knowing about intelligence.

The scale and complexity of the threats to national security from terrorism are continuously evolving. Therefore, counter-terrorism measures also need advancement to seek new ways to pursue progressive developments. Harnessing the power of OSINT continues to be a game-changer for intelligence community. In this context, developed countries established dedicated OSINT centres i.e. Defence Open Source Council (DOSC) (US), OSINT Hub (UK), DGSI OSINT centre (France), OSINT centre CSIS (Canada), etc.[2] The purpose of this paper is to explain the importance of OSINT in the context of counter-terrorism which has become crucial for national security. The problem is approached by establishing linkages between the security triad – National Security, Counterterrorism, and Open-Source Intelligence. It concludes with the argument that OSINT has an integral place in National Security in the 21st century.

ROLE OF COUNTER TERRORISM IN NATIONAL SECURITY OF PAKISTAN

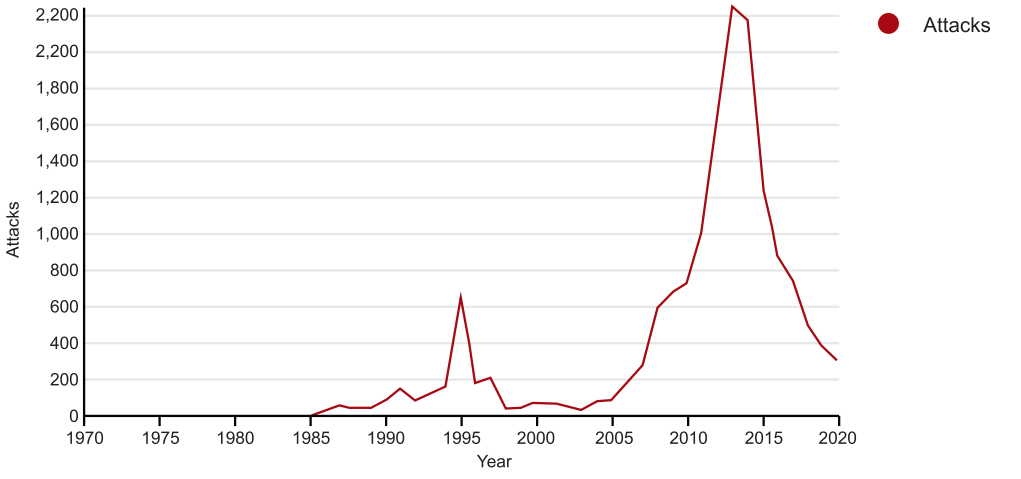
In National Security Policy (2022-2026), the government recognized terrorism as the most acute form of effort to undermine stability and national harmony. Terrorism is a global issue, NSP prioritizes the conduct of Intelligence-Based Operations (IBOs) against all terrorist groups, preventing any deprivation in recruitment areas, and promoting a pluralistic anti-terror narrative. However, it has become challenging to solely rely on traditional means since the evolving technology is being exploited by terrorist organizations. The existing

1 Kim R. Holmes, "What is National Security?," *US Military Strength Index,* 2015: 18, https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf

2 Akhgar, Babak, P. Saskia Bayerl, and Fraser Sampson, eds. *Open-source intelligence investigation: from strategy to implementation.* Springer, 2017.

transformation in information space due to wide use of internet and social media necessitate a response in the same domain - OSINT.

Terrorist Incidents - Pakistan



Source: Global Terrorism Data Base[3]

DEFINITIONAL SHORTCOMINGS OF OSINT

OSINT lacks a commonly shared definition. Generally, it can be defined as, "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience to address a specific intelligence requirement."[4] US National Defence Authorization Act 2006 also agree with this definition in section 931(1)(a).[5] Following the official NATO terminology database, OSINT is intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access. Schaurer, Florian, and Jan Storger define OSINT as "a process by which publicly available information is transformed into actionable information through proper processing and analysis".[6] However, Heather J.

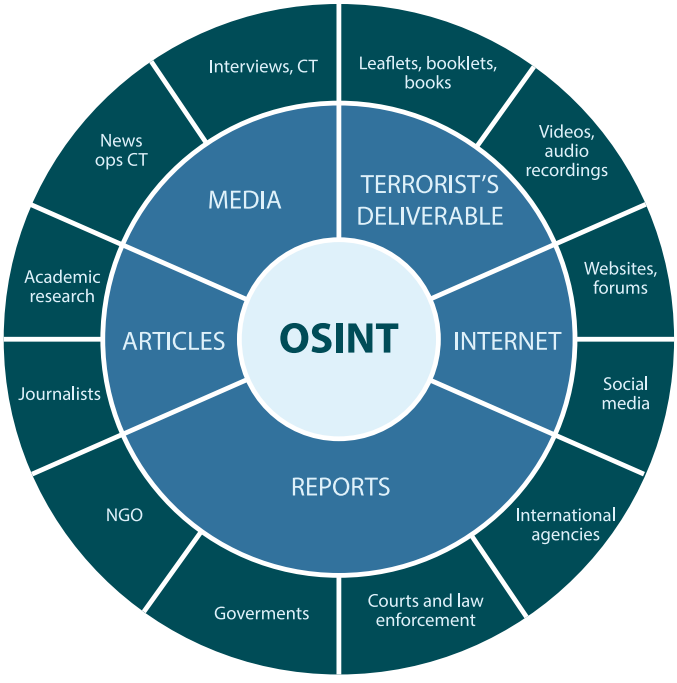
3 "Pakistan Terror Attacks Database," *Global Terrorism Database,* 2022, https://www.start.umd.edu/gtd/search/Results.aspx?search=Pakistan&sa.x=0&sa.y=0

4 Roger Z. George and Robert D. Kline, Intelligence and the National Security Strategist: Enduring Issues and Challenges (Rowman & Littlefield, 2005): 119.

5 "National Defense Authorization Act For Fiscal Year 2006," Gov.info, (2006): 277, https://www.*Gov.info,* gov/content/pkg/PLAW-109publ163/pdf/PLAW-109publ163.pdf

6 Schaurer, Florian, and Jan Störger. "The evolution of open source intelligence (OSINT)." *Comput Hum*

Williams, and Ilana Blum argued that OSINT should be seen as second-generation OSINT, after significant transformation of the Internet and the rise of social media. OSINT has become more complex in terms of both sources and methods.



Source: Variety of Open Sources[7]

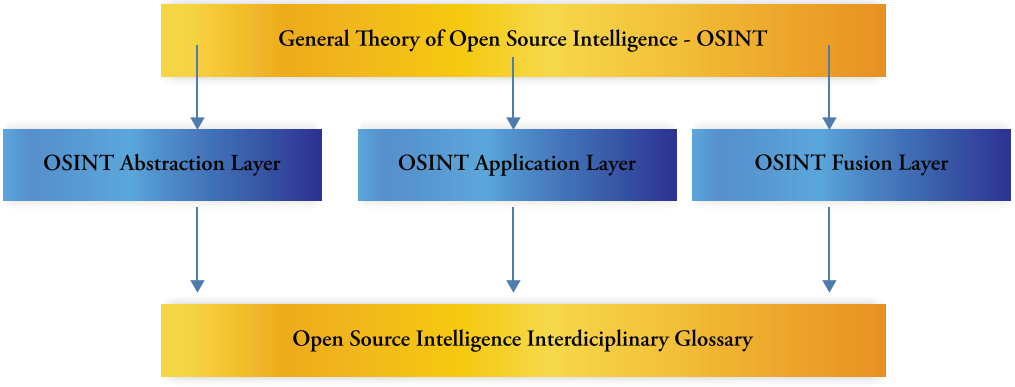
Since this paper is not intended to expound on a definition of OSINT or its flaws, therefore, it is based on NATO's definition of OSINT along with the non-intrusive part of SOCMINT. However, OSINT is required to be defined at a national level as a practice of accessing the information of public character - without compromising privacy, laws, patents, and copyrights.

Behav 19 (2013): 53-56.

7 For figure, see Ensar Seker, "Open Source Intelligence 101," Data Driven Investor, July 08, 2020, https://medium.datadriveninvestor.com/open-source-intelligence-osint-101-d96f47ff2ff1 . For detailed study, see Nihad A. Hassan and Rami Hijazi, *Open Source Intelligence Methods and Tools* (Berkeley, CA: Apress, 2018)

GENERAL THEORY OF OSINT

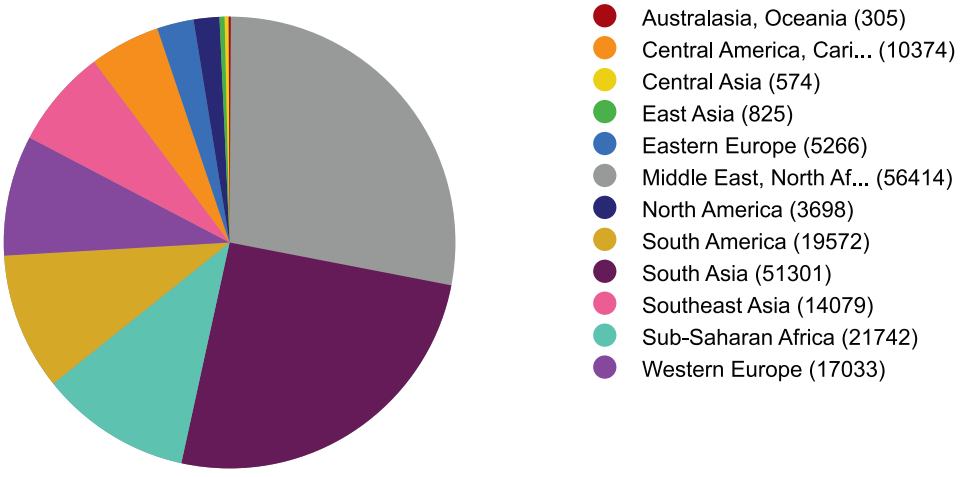
Giovanni Nacci, an Italian OSINT expert since 1998, advocated the General Theory of OSINT (GT/ OSINT). His work provides the required conceptual interfaces between OSINT, intelligence studies, and many other disciplines that can contribute to the strengthening of OSINT theoretical framework. GT/ OSINT constitute 'Layer Trilogy' i.e., Abstraction Layer, Application Layer, and Fusion Layer. He posits OSINT as a separate discipline rather than a technique augmenting traditional intelligence, places it as ontologically superordinates to all the other forms of classified intelligence, and emphasizes fully available and accessible information. OSINT is much more akin to source than information i.e., intelligence about the source is preferred over intelligence from the source.



Source: General Theory of OSINT[8]

The combined effect of OSINT and traditional intelligence sources reflects national security intelligence apparatus in the 21st century. OSINT provides context and fill the gaps for classical intelligence which reaffirms the theory to view OSINT as superordinate. George F. Kennan, an experienced US government official, and historian wrote to US Commission Chairman Senator, that "95% of what we need to know could be very well obtained by the careful and competent study of legitimate sources of information, open and available". After that in Dec 2005, former Deputy Assistant Director of CIA, W.M. Nolte stated that 95–98% of all information handled by the US intelligence community derives from open sources.[9]

8 Giovanni Nacci, "General Theory of Open Source Intelligence in Brief," *Intelli|sfèra*, August 2019: 01.
9 Christopher Hobbs, Matthew Moran, and Daniel Salisbury, eds., *Open Source Intelligence in the Twenty-First Century* (London: Palgrave Macmillan UK, 2014), https://doi.org/10.1057/9781137353320.



Source: Global Terrorism Data Base[10]

INTERNET EXPLOITATION BY TERRORISTS

Social media and the surface web are used fundamentally for psychological, moral, and emotional tactics. The dark web is used to a greater degree for the physical and tactical side of operations, focusing on arms and munitions, false documents, explosive-making guides, crypto currency funding, and encrypted anonymous strategic communications.[11] Besides dark web, open sources are now increasingly being used by terror outfits to project their ideologies, to spread misinformation, to stir destabilizing emotions in times of crisis, and promote their recruitment drive. Similarly, on the opposite axis, OSINT can offer a critical ability for LEAs to complement their intelligence to fight terrorism.

OSINT APPLICATION IN COUNTER TERRORISM

Terrorism is an unlawful use of violence and intimidation, especially against civilians, in pursuit of political aims. Motives are to instil fear and uncertainty, to achieve maximum publicity for explicit objectives. In view of Crenshaw (2004), protest pushed into violence is the consequence of two affecting factors; preconditions, or circumstances that encourage

10 Global Terrorism Database, "*GTD Search Results*," https://www.start.umd.edu/gtd/

11 Babak Akhgar, P. Saskia Bayerl, and Fraser Sampson, eds., *Open Source Intelligence Investigation: From Strategy to Implementation*, Advanced Sciences and Technologies for Security Applications (Cham: Springer International Publishing, 2016), https://doi.org/10.1007/978-3-319-47671-1.

an incentive to resort to violence.[12] This means that LEAs are required to monitor the circumstances leading to terrorism, and the internet could not be ignored. The combined effect of OSINT and traditional intelligence sources reflects national security intelligence apparatus. However, OSINT is superordinate to classical intelligence as per GT/OSINT. OSINT provides context and fills the gaps for classical intelligence which reaffirms the theory to view OSINT as superordinate.[13]

COMPREHENSIVE SECURITY

The theory of securitization given by Barry Buzan conceives the multi-layered nature of contemporary security i.e., economic, political, societal, military environmental, etc. It strives to develop a complete understanding of interlinking concept of people, state, and fear.[14] This web of interconnected factors helps us develop a cohesive overview of national security. The broadening of the security agenda has raised the demand for more information, which in turn has fostered a growing appreciation of the value and utility of OSINT.

EMERGING TECHNOLOGIES

The proliferation of websites, portals, wikis, and blogs has opened a world of information hitherto unavailable to most intelligence professionals.[15] The use of open-source intelligence gathering for national security dates to the cold war era. However, OSINT in 21st century has become crucial as 'one to many' communication models has been shifted to 'many to many and the receiver of information has also become the transmitter. Moreover, internet has become first platform for onlooker to gain an understanding of happenings around him/her. Therefore, it serves malicious agendas against the state to affect public perception. Critical theory of emerging technologies helps understand exploitation of new technologies for contextualization. While reconceptualization to de-contextualization in this regard, following are some recent examples of OSINT effectiveness amongst many:

12 David J. Whittaker, *Terrorists and Terrorism in the Contemporary World*, 2004th ed. (Routledge 11 New Fetter Lane, London EC4P 4EE, n.d.).

13 Christopher Hobbs, Matthew Moran, and Daniel Salisbury, eds., *Open Source Intelligence in the Twenty-First Century* (London: Palgrave Macmillan UK, 2014), https://doi.org/10.1057/9781137353320.

14 Barry Buzan, "People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era",(ECPR Press, 2008).

15 Chris Pallaris, "Open Source Intelligence: A Strategic Enabler of National Security" (Research Paper, Center of Strategic Studies, 2008), file:///E:/OSINT%20-%20IRP/OSINT%20Strategic%20Enabler%20of%20NS.pdf.

RUSSIA - UKRAINE CONFLICT

OSINT has given Ukraine an edge both militarily and politically. This edge has allowed Ukraine to withstand Russia's assault.[16] Politically, OSINT has been exploited to swing international opinion in favor of Ukraine by removing the fog of war. Militarily, OSINT has allowed the Ukrainian military to track Russian military movements, plans, and operations by exploiting satellite pictures. Moreover, OSINT analysis has become a normal part of US and European news reporting related to Ukraine.[17] OSINT is also being applied using geo-location tools to track the trapped students to rescue in real-time against Russian air-raids and ground troop activity.[18]

COORDINATED GLOBAL TWITTER CAMPAIGN – '#SANCTION PAKISTAN'

OSINT analysts of Project Baseerat, a non-profit firm of volunteers in Pakistan, traced the origins of anti-Pakistan campaign which became a top trend on Twitter in August 2021 after the Taliban took over Afghanistan i.e. '#Sanction Pakistan'.[19] The investigation revealed that the campaign was started by an Afghanistan based fake/ controlled account in March 2021. Moreover, former Canadian diplomat and politician Chris Alexander was the first verified person who used it. Afghan government officials with verified Twitter accounts actively participated in this campaign. Investigations revealed that Afghan ambassadors posted in UAE, Sri Lanka, and Czech Republic used this hashtag in their tweets in March 2021.

INFORMATION SECURITY AND PERCEPTION MANAGEMENT

The surveillance of community through OSINT has become imperative. Owing to exponential rise in internet users and their duration online, there are numerous sources

16 Vanessa Smith Boyle, "How OSINT has shaped the War in Ukraine," American Security Project, June 22, 2022, https://www.americansecurityproject.org/osint-in-ukraine/

17 Matt Freear, "OSINT in an Age of Disinformation Warfare," *RUSI*, March 14, 2022, https://rusi.org/explore-our-research/publications/commentary/osint-age-disinformation-warfare

18 Gabriel Geiger, Inside the OSINT Operation to get Foreign Studnets out of Ukraine," *VICE News*, March 12, 2022, https://www.vice.com/en/article/epx88p/inside-the-osint-operation-to-get-foreign-students-out-of-ukraine

19 Zaki Khalid, "Examining the Coordinated Global Twitter Campaign 'Sanction Pakistan'," Project Baseerat, August 11, 2021, https://www.projectbaseerat.com/2021/08/11/examining-the-coordinated-global-twitter-campaign-sanction-pakistan/

of intelligence extraction as well as perception management. By monitoring the flow of data, analysts can identify the trends in real-time. OSINT can help the identification of terrorist networks, their narrative builds up, and rapidly support identification of radical roots within online communities. It reveals terrorists propaganda, deception, disinformation, and misinformation. Therefore, OSINT significantly enhanced the capabilities to identify planning of attacks and spot the early signs of radicalization and recruitment.

OSINT LINKAGES WITH NATIONAL SECURITY

NSP (2022-26) identified national cohesion as the guiding principle for 'unity in diversity'. OSINT is vital for national cohesion being the only instrument for monitoring online content. US CIA Director has argued that a proper analysis of intelligence obtainable by overt means supply over 80% of information required for the guidance of national policy.[20] The argument was considered null and void before the 'Big data' revolution when open source data was very limited. Therefore, OSINT can play an effective role in 'national cohesion' which is significant for counterterrorism. Leading economic cum political powers are using various OSINT tools for counter-terrorism. However, data for same is not available in Open-Source. Analysis of one reliable counter-terrorism – '4P Contest' model of the UK in coherence with OSINT may help to devise need-based OSINT system.

OSINT PROPOSITION – 4P CONTEST

4P CONTEST model is United Kingdom's strategy for Counter Terrorism enforced in June 2018. Efficacy of OSINT for counter-terrorism has been shown by validating its application on CONTEST framework. Moreover, OSINT has also been pitched for relevant agendas of Pakistan's recent national security policy for countering terrorism and extremism. OSINT is weighed against each 'P' of CONTEST strategy to validate its application for counter-terrorism. An overview of the four principles and how OSINT may be employed in their support is given below:

Prevent

The Prevent strategy is concerned with tackling the radicalization of people who sustain the international terrorist and organized crime threat. OSINT is applied in identification

20 Christopher Hobbs, Matthew Moran, and Daniel Salisbury, eds., *Open Source Intelligence in the Twenty-First Century* (London: Palgrave Macmillan UK, 2014), https://doi.org/10.1057/9781137353320.

of terrorist narratives, influencers, and propaganda over the surface web, particularly in countering attempts to turn people to terrorism by 'incitement and recruitment.[21] Therefore, OSINT may be exploited in tackling the factors or root causes that can lead to radicalization and recruitment/ by causal process tracing. After valuable input from OSINT to decision-makers, a more effective counter-extremist narrative may be formed. Online monitoring of society provides aid to decision-makers in understanding the communities and areas of concern.

Pursue

The Pursue strategy is concerned with reducing the terrorist threat by disrupting terrorists and organised criminal groups along with their operations[22]. OSINT is applied at operational/ tactical level in gathering intelligence from the dark web. The legal and ethical collection of evidence for securing international cooperation may help to pursue and investigate terrorist threats. As OSINT evidence can be reproduced for litigations, OSINT may also augment the efforts of LEAs to impede the travel and communication of terrorists and criminals. It will precisely support to disrupt their networking, funding, access to attack materials, and to bring individuals to justice.

Protect

OSINT is an aid for proactive threat assessment of vulnerabilities (e.g., border security) and social areas of risk. Proactive and live assessment of threats to mass gatherings may also be monitored online through various tools and techniques[23]. Therefore, 'Protection' of National Critical Infrastructure (NCI) i.e., cyberspace, and reduction of its vulnerability to attacks will further depend upon OSINT application.

Prepare

The Prepare strategy is concerned with ensuring that the population is as ready as it can be for the consequences of terrorist attacks and organised criminal events. Threat mitigation may be improved in domain of OSINT by threat perception and prospect risk calculations. In this objective, OSINT may be implied to identify shortcomings and provide a way ahead.

21 Akhgar, Bayerl, and Sampson, *Open Source Intelligence Investigation*.
22 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.
23 Hassan and Hijazi, *Open Source Intelligence Methods and Tools*.

OSINT CENTRIC HUB

The Centre of Excellence in Terrorism, Resilience, Intelligence, and Organised Crime Research (CENTRIC) has built a strong research and development capability focused on the operational utilization of OSIN.[24] The study of model depicts a close collaboration of organization with national, pan-European, and international partners in academia, public and private sectors. Counter-terrorism strategy requires a wholesome approach and global collaboration to effectively deal with emerging threat

DIMENSIONS OF ONLINE RADICALIZATION

National security is troubled by unchecked availability of youngsters who are prone to radicalization. The first step to be considered for social reconstruction is deradicalization as "radicalization is the process of causing someone to adopt radical positions on political or social issue".[25] Post-9/11, terrorism has rapidly spread, through exploitation of vulnerable people. Globally, there are growing concerns that citizens are being hired, radicalized, trained, and tasked online in an ungoverned virtual domain. The Foreign Policy Research Institute of United Kingdom evaluates that between 6000 - 12,000 Daesh online inspired volunteers have passed through Syrian territory, refugee/unregistered influx from 70 different countries.[26] The interconnected and globalized world facilitates terrorist organizations to attract a large pool of individuals

CYBER PSYCHOLOGY

The internet helps terrorist organizations to amalgamate radical ideas as social norms i.e., the use of violence to address grievances. It is important to identify the causes of grievances that might be exploited by hostile elements. People have adopted the change and easier option of surfacing grievances online with more impact and coverage. A tweet spread amongst millions in a matter of few minutes and pass on the idea across the globe. It is very important to recognize that terrorist groups can exploit vulnerabilities by giving a clear sense of identity and ownership.[27] Individuals considered at potential risk of radicalization share a sense of injustice which may be traced from their online footprints very easily.

24 Akhgar, Bayerl, and Sampson, *Open Source Intelligence Investigation*.
25 Ana Sofia Florez, "Radicalization through Internet: How ISIS Became so successful and why United States needs to catch up," *International Studies*, May 18, 2019.
26 Akhgar, Bayerl, and Sampson, *Open Source Intelligence Investigation*.
27 David J. Whittaker, *Terrorists and Terrorism in the Contemporary World*.

ONLINE FOOTPRINT OF RADICALISATION

Physical radicalization of an individual may be subtle, while his online traces may be more visible as people generally feel secure in anonymous use of internet. Identifying radicalization remains the main task of intelligence community for earlier prevention. As online radicalization has not only targeted people but also communities, through psychological reengineering.

OSINT - COUNTER MEASURE TO ONLINE RADICALISATION

The advanced nations have devised mechanisms to collect valuable information about communities, and vulnerabilities to extremist recruitment and radicalisation. For instance, the establishment of CENTRIC OSINT Hub by United Kingdom since 2012.[28] Intelligence communities have traditionally played an important role to measure vulnerabilities in society that may be exploited. Thereafter, decision-makers utilize vital information and endeavor to draw goodwill from a vulnerable portion of society. The next step is to find the potential or existing threats of exploiting those vulnerabilities to achieve their objectives i.e., psychological operations, narrative building, radicalisation, recruitment, etc. The counter-strategy hinges upon coordination between LEAs and Intelligence Community in which the information is to be shared on a 'need to share' approach rather than a 'need to know approach. The purpose of collaboration is a relentless pursuit to gather information and proactively read the terrorist covert designs. An important aspect of gaining intelligence through open source is social media in which the user not only receives information but recreates, reshapes, and re-shares it.

IMPERATIVE IN 21ST CENTURY

The surveillance of community through OSINT has become imperative. Owing to exponential rise in internet users and their duration online, there are numerous sources and data for intelligence extraction. By monitoring flow of data, analysts can identify the trends in near-time.[29] In context of counter-terrorism, OSINT can help the identification of terrorist networks and rapidly support the identification of radical roots within online communities. It can provide significantly increased capabilities and opportunities not just to prevent terrorist

28 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.

29 Nihad A. Hassan and Rami Hijazi, *Open Source Intelligence Methods and Tools* (Berkeley, CA: Apress, 2018), https://doi.org/10.1007/978-1-4842-3213-2.

attacks, but to identify attack planning activity. Most importantly, it can spot the early signs of radicalization and recruitment to stop violent and extremist development at source. It reveals terrorist's propaganda, deception, and misinformation. Moreover, countermeasures can be generated and applied to nullify or debunk such propaganda campaigns being run by hostile elements. In sum, the following key points regarding OSINT can be highlighted:

- Information space has immensely evolved due wide use of internet and social media.
- The evolving technology has been exploited by terrorist organizations which necessitate a response in same domain.
- LEAs are required to monitor the circumstances leading to terrorism and internet could not be ignored in on-going information age.
- Terrorists use social media and surface web for psychological, moral, and emotional tactics and the dark web for physical and tactical operations.
- OSINT is a means of providing context for further intelligence and filling the gaps of classical intelligence at later stages.
- OSINT needs a proper definition/recognition at a national level for accessing information of public character without compromising privacy laws, patents, and copyrights.
- The demand for more information security in NSP has fostered the value and utility of OSINT.
- Online traces of radicalisation are more prominent as compared to an apparent, due sense of security and anonymous identity.
- OSINT reveals terrorist's propaganda, deception, and misinformation.
- Individuals considered at potential risk of radicalization share a sense of injustice which may be traced from their online footprints very easily.
- People have adopted the change and easier option of showing grievances online with more impact and coverage.
- OSINT can play an effective role towards 'national cohesion' which is significant for counter-terrorism.

OPERATIONAL CYCLE

OSINT is underutilized due to difficulty in understanding of sources and methods, particularly social media platforms.[30] Extracting valuable intelligence from Big Data - 'huge

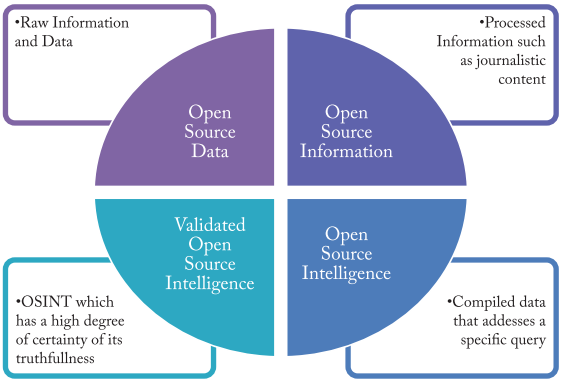
30 Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*.

in volume and growing exponentially with time' is like drinking water from a fire hydrant. Interviews and literature reveals two methods of OSINT, manual (without tools – more reliable but time-consuming) and semi-automatic (less time-consuming as well as reliable). There must be some funnel to cater the pressure of hydrant to make it possible to drink the water i.e., tool. The second challenge is reliability and accuracy of data, which involves strategic techniques. Therefore, OSINT is not simply 'web surfing, there is a complete process involved - OSINT operational cycle. The operational cycle of OSINT is the way to utilize the 'Big data' for intelligence purposes involving under-mentioned steps/ techniques.

FROM DATA TO OSINT

Before embarking on the process, it is important to distinguish between information and intelligence which are often misunderstood as similar concepts. However, a careful examination reveals a subtle distinction; when information is treated with detailed analysis and processing, it becomes intelligence. In this context, when such information is collected from public sources, the product is called OSINT.[31] NATO splits open-source information and intelligence into four categories given below.

Process to Validated OSINT

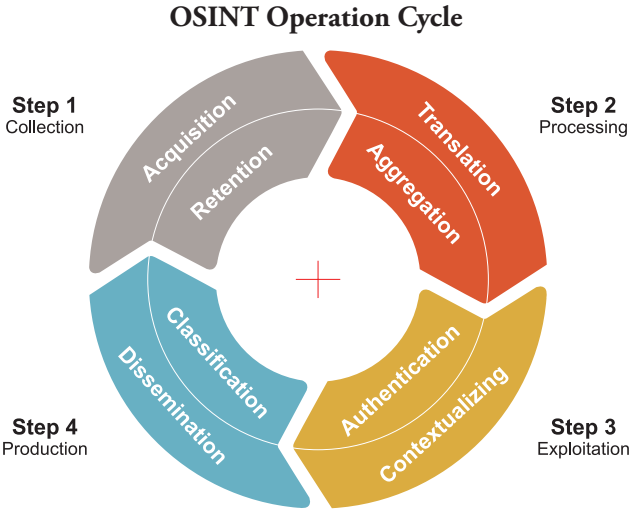


Source: Open Source Intelligence Investigation[32]

31 Akhgar, Bayerl, and Sampson, *Open Source Intelligence Investigation*.
32 Akhgar, Bayerl, and Sampson, *Open Source Intelligence Investigation.*

METHODOLOGY

In OSINT, four key steps are focused on: collection, processing, exploitation, and production.[33] In the simplest terms, the process can be described as acquiring information, validating that information, and passing it to decision-makers.



Collection

The first step is the identification of potentially useful information. That means the collector is clear in his mind about what he must collect.[34] Prior internet, the collection process required physical reach to the location. However, logistic challenges in physical movement have shifted from processing to information management. It means a collection of data is easier and cheaper in OSINT.

Processing

Processing involves validating the information and making it usable.[35] It may include translating and transforming content to usable intelligence. Processing in second-generation OSINT has shifted to software programs; however, interviews with practitioners revealed

33 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.
34 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.
35 Hassan and Hijazi, *Open Source Intelligence Methods and Tools*.

that many good analysts prefer manual processing for more credibility.

Exploitation

Exploitation seeks to determine whether the information is what it purports to be and what its value is to the Intelligence Community.[36] One of the most significant challenges is the degree of reliability inherent in that information.[37] It is time taking and difficult step, especially in social media where tools have limitations due to emotions involved and unstructured language.

Production

Production is the provision of information to consumers in usable form.[38] The consumer is a source analyst who counter-checks the information and assigns an admiralty code before dissemination.

STRATEGIES FROM ACQUISITION OF DATA TO INFORMATION EXTRACTION

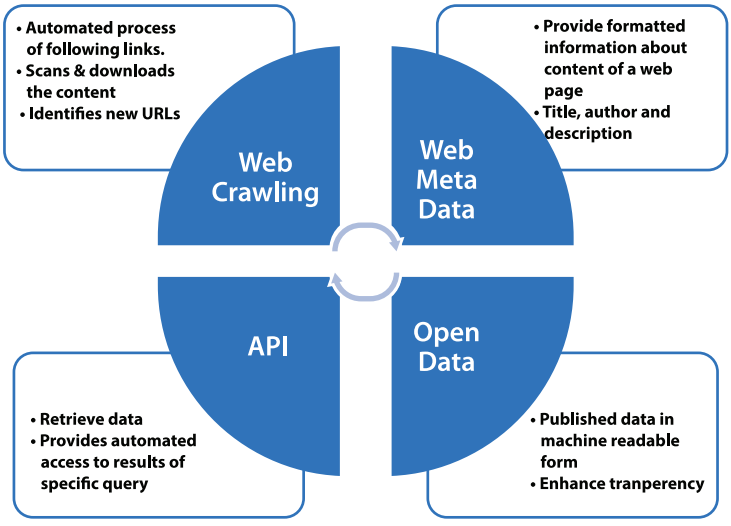
OSINT has numerous sources; therefore, analysts take support of various AI tools to speed up the process. The challenge of collection is different for different types of data i.e., structured, semi-structured, and non-structured data. Subsequently, the information extraction stage is also automated through use of various tools.

AUTOMATED SEARCH TECHNIQUES

It is cumbersome task for an individual to troll through checking one site to another for the desired information. In this regard, automated search techniques are widely used. There are variety of techniques available. An overview of few imperative techniques is given in the figure below.

36 Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*.
37 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.
38 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.

Automated Search Techniques



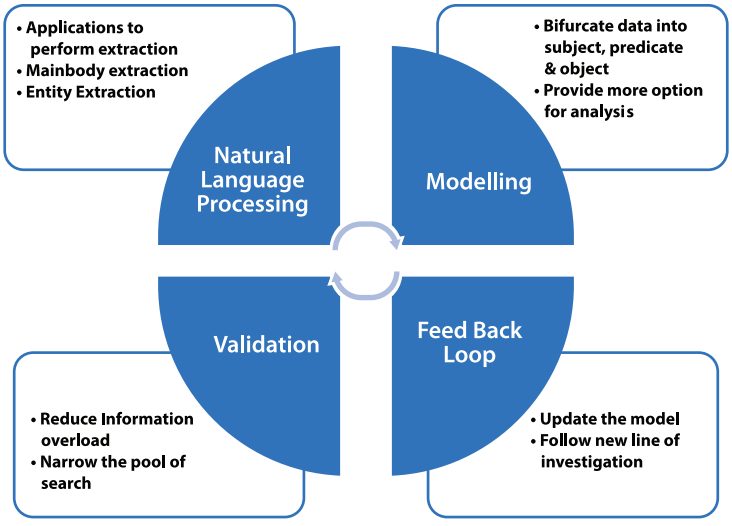
Source: Open Source Intellegence in 21st centuary[39]

INFORMATION EXTRACTION

The process of converting data from an unstructured state into a structured state is called Information extraction.[40]An overview of few information extraction techniques is given below.

39 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.
40 Akhgar, Bayerl, and Sampson, *Open Source Intelligence Investigation*.

Information Extraction Process



Source: Open Source Intelligence in the Twenty-First Century[41]

ADVANTAGES OF OSINT

OSINT is low cost in both collection and sharing, therefore, more suitable for developing countries. OSINT is collected using ethical means, therefore, it can be used in legal proceedings. Information gathering through OSINT is risk-free as compared to spies or other clandestine means used in close means. It provides context and validation for traditional sources.

INCIDENT MONITORING AND RESPONSE

The disruptive programmes organised by mobs with violent tendencies vehave become regular feature in Pakistan i.e. protests, demonstrations, etc., and is widely covered on social media through unique hashtags to popularise the agenda and coordinate. OSINT has potential to extract the content from specific geolocation to prompt the concerned authorities. OSINT also provides an opportunity to mark the main igniter/ planner of such activities by monitoring social media.

41 Hobbs, Moran, and Salisbury, *Open Source Intelligence in the Twenty-First Century*, 2014.

TRACKING NARRATIVE BUILD-UP

The report of EU Dis Info Lab on Indian chronicles – 15 years of influence operations for anti-Pakistan narrative building was revealed through OSINT. Therefore, it indicated strategic importance of OSINT to National Security. Moreover, it is also helpful in monitoring malicious and aggressive designs at domestic level. By analysing the propagation pattern of online content and the originator (source of hashtag), the chain of influential distributors can be tracked and identified. Such accounts may be placed under a watch list by relevant authorities.

OPPORTUNITIES FOR PAKISTAN

As per PTA report of January 2022 internet users in Pakistan reached a figure of 113 million with penetration rate of 51.28% as compared to 27.5% in 2021.[42] More internet users enhance the effectiveness as well as need for OSINT.

S No	Social Media	Users (Millions)
1	Facebook	43.55
2	You Tube	71.7
3	Instagram	13.75
4	Tik Tok	18.26
5	Facebook Messenger	12.6
6	Linkedln	7.6
7	Snapchat	18.8
8	Twitter	3.4
9	Mobile connections	186.9

Table 1 World Digital Portal Jan 2022[43]

Recently, a pioneer private registered firm under the name 'Pantellica' started the conduct of OSINT course in Islamabad.[44] Moreover, an international training and consultancy group

42 Simon Kemp, "Digital in Pakistan: All Statistics you need in 2021," *Data EPortal*, Feburary 11, 2021, https://datareportal.com/reports/digital-2021-pakistan#:~:text=There%20were%2061.34%20million%20internet,at%2027.5%25%20in%20January%202021.

43 Ibid.

44 "Pantellica – Empowering through Intelligence," https://pantellica.com/

– Nobel Group is also conducting online OSINT courses.

S No	Institution	Course	Cost
1	Pantellica	OSINT Basic	Starts at 600 USD
		OSINT Advance	Starts at 1800 USD
2	Nobel Program (Online only)	OSINT Basic	Starts at 470 USD
		OSINT Advance	Starts at 1500 USD

Table 2 OSINT Courses in Pakistan

Free courses of Artificial intelligence (Machine Learning and Deep Learning), Advanced Data Analytics (NLP), and Advance Python Programming and Application by government under Kamyab Jawan Program, indirectly contribute towards OSINT skill development.

CONCLUSION

The broadening of security agenda has raised demand for more information, which in turn has fostered growing appreciation of the value and utility of OSINT. The nexus in trilogy of national security, counterterrorism, and Open-Source Intelligence is important. OSINT is important for Pakistan's aspirations to prevent vulnerabilities and to guide the counter-narrative. The national policy of Pakistan identifies a preventive approach to counter-terrorism and builds an anti-terror narrative. OSINT provides ways to achieve the objectives of National Security Policy of Pakistan, prove pivotal towards national security. OSINT can potentially provide critical capability for LEAs and security services to complement and enhance their intelligence capability. The successful implementation of the CENTRIC OSINT Hub is an example of how academia and LEAs can collaborate within the OSINT sphere to bring research into reality for the security and protection of citizens. The process of data collection and information extraction is tedious and long. However, it is cheap and just need expertise to develop such tools.

RECOMMENDATIONS

For Policy Makers

Policymakers need to establish a National OSINT centre in line with contemporary models under Federal authority to provide access to all LEAs in the country. Thereafter, the requirement of training to produce OSINT analysts must be organized. The next challenge would be its data cloud. Therefore, initiatives are to be undertaken for the development of a National data bank of open-source intelligence. Concrete steps towards progress on OSINT cannot be achieved without collaborations with similar OSINT entities. Meanwhile, supervise out-sourced services; training sessions and seminars at a local level will be required for awareness on subject. Establishment of Provincial OSINT centres under the ambit of National OSINT centre are crucial to create synergy at national level.

Since terrorism is a global problem, therefore, government needs to adopt a wholesome approach to Counterterrorism. This can be done through close collaboration and cooperation with organizations (National and International partners) in academia, public and private sectors. Meanwhile, legislation should be done for the regulation of OSINT centres, the legal value of OSINT-based information, and its institutionalization. For legislation, there is requirement of formulating OSINT definition at National level, defining its scope, and limits for accessing the information of public character without compromising privacy laws and copyrights. Moreover, OSINT should be included in Higher Education Commission research priority areas. Preferential tax regimes (tax rebates) may be introduced to attract investment in private OSINT firms and institutions. Government should include the basic and advanced courses of OSINT under Kamyab Jawan Program free education system.

For LEAs

Training of personnel under their own resources for establishment of dedicated setup to detect threats to 'national cohesion' which is significant for counterterrorism is a short-term solution for LEAs. Formulation of avenues for collaboration with academia and industry to highlight OSINT-related requirements for research and development need prioritization. Effective lobbying would be required to unite the public and private sectors, communities, citizens, and overseas partners to establish OSINT centres.

Meanwhile, efforts are required to exploit OSINT - to monitor the circumstances

leading to terrorism i.e., online radicalization, psychological operations, and propaganda. It would provide means for online monitoring of society (social perception), to provide aid to decision makers for understanding the communities, and areas of concern. LEAs may exploit OSINT for proactive and live assessment of threats to mass gatherings through various tools and techniques. LEAs should prefer a manual method of OSINT - till development of tools by their experts, due to security reasons as well as ineffectiveness of foreign tools in our environment. LEAs should conduct a comparative analysis of 4P CONTEST model of counter-terrorism with existing model in Pakistan.

For Academia

Academia should collaborate with private OSINT institutions, such as, Project Baseerat' and Pantellica, for research and development in OSINT. Meanwhile, continued efforts are needed, for lobbying and making OSINT a recognized discipline of study in educational institutions. Similarly, MoUs with reputed international firms conducting OSINT courses should be pursued. Conduct of future studies on methods, tools, and techniques of OSINT, and existing potential for OSINT by surveying the available data analysts and machine language experts, etc., can be done.