Rising Role of OSINT in Conflict/War

Sanjay P Vishwasrao

"OSINT provided roughly 90 per cent of the information used by intelligence community."[1]

—Lt Gen Samuel V Wilson, ex-Director US DIA

Abstract

Information and communication technology, the internet of things, and cellular networks have colluded with smartphones in the hands of globalised humans to change the character of war. Consequently, Open-Source Intelligence (OSINT) has emerged as the key driver of the intelligence acquisition cycle, with citizens and corporates involved alongside the militaries. Ongoing wars in Ukraine and Israel have exposed the link of social media with intelligence, strategic communication and cyber warfare. This new form of OSINT with a high level of civil-military synergy is making major contributions in all periods of conflict, stages of war, and spectrums of war. In order to secure India's interests, while it leaps forward to a US$ 10 trillion economy India needs to structure and strategise to win every technology drive competition in peace and war. Exploiting and defending against OSINT has thus become a key security necessity of our times.

Major General **Sanjay P Vishwasrao**, SM and bar, is a serving Army officer who has been a Defence & Military Advisor in High Commission of India, Pakistan. Views expressed are personal.

OSINT Revolution

Open-Source Intelligence (OSINT) a.k.a 'White Intelligence' has captured the eyeballs of political leaders, generals, soldiers, netizens and citizens because of the ongoing world's 1st Digital War in Ukraine. It is also being called the 1st social media war, like the Spanish American War of 1898 was called the 1st media war, the Vietnam War the 1st televised war and Arab Spring the 1st internet war.[2]

The proliferation of smartphones with up to 30 sensors in each, globalisation induced rising human interest in geo-strategy and homeland security, and human addiction to social media applications has triggered an OSINT Revolution.

This (re)awakening to the relevance of OSINT was bound to happen. Ushering of 2nd Generation OSINT (1st Generation was from 1940 to 2008) has happened due to the paradigms of information communication technology (ICT), internet-of-things (IoT), cellular telephony and smartphones with an ever-growing number of applications.[3] The proliferation of smartphones with up to 30 sensors in each, globalisation induced rising human interest in geo-strategy and homeland security, and human addiction to social media applications has triggered an OSINT Revolution. Every citizen with a smartphone is not only a soldier but is also a sensor.[4] The battlefields of the 21st century are full of eyes and ears, be it soldiers themselves using social media or ordinary citizens with smartphones. Social media today is at the cutting edge of the intelligence cycle i.e., detect/find targets i.e., open-source information data (OSD) and open-source information (OSINFO) for subsequent analysis and engagement. Crowdsourcing of OSINT provides intelligence operatives the opportunity to monitor events, collect information and assess the enemy's preparedness in real-time for battlefield transparency (BFT).

The flip side is that, planned 'event barraging'[5] (deception) can lead to wrong OSINT pieces being fitted into the jigsaw puzzle. The October

7, 2023 Hamas attack on Israel is a perfect example of this OSINT Trojan Horse a.k.a Black Intelligence. The collusion between state, military, intelligence agencies, citizen social media users, and commercial ICT and IoT companies is a wake-up call for practitioners of national security. A balanced evaluation of OSINT would list its advantages as low cost, high speed, good quality, variety of sources, low risk to the life of agents, automation of analysis and ease of sharing across borders. The drawbacks are a huge quantity of information and weaponisation for deception/ disinformation and for subversion/corruption of the intelligence cycle (Plan-Acquire-Process-Analyse-Disseminate loop) and the command cycle (Observe-Orient-Decide-Act loop). The 'whole-of-nation' (Israel) or 'whole-of-religion' (Hamas) or 'whole-of-alliance' (NATO vs Russia) approach to conflicts and wars is leading to global marshalling and weaponisation of OSINT sources. A large percentage of OSINT actors on both sides of the conflict may not reside in the battle space/war zone. Thus, rendering them ineffective is impossible within the limits of international laws.

In spite of the double-edged nature of OSINT, unclassified information is now seen as much more than supplementing classified information i.e., human intelligence (HUMINT) and technical intelligence (TECHINT). Triangulation for corroboration within and among OSINT, HUMINT and TECHINT is the new rule of the game.[6] So, while OSINT may appear to have reduced the fog of war, it has definitely increased the friction in war.

Ocean of OSINT

As per General Anthony Zinni (former commander of US Central Command), "80 per cent of what I needed to know as CINCCENT, I got from open sources rather than classified reporting. And within the remaining 20 per cent if I knew what to look for, I found another 16 per cent. At the end of it all, classified intelligence provided me, at best, with 4

per cent of my command knowledge."[7] Open sources are comparatively richer in data in today's flat interconnected globalised world. OSINT sources/techniques are broadly classified as offline and online. Offline ones are diplomatic, academic, corporate and mass media. Online sources are social media mining, website analysis, geo-location, image analysis, network analysis, e-mail analysis and dark web analysis. OSINT process flow to exploit these online and offline sources is: to identify the source, harvest data, process data, analyse information, and report and disseminate assessments. The success of OSINT depends on the use of disparate sources of open-source data (OSD), investigation of the dark web, and use of appropriate software, artificial intelligence (AI) and machine learning (ML). In addition, due to the short life span of OSINT, the intelligence cycle has to be continuous and repetitive.[8]

The success of OSINT depends on the use of disparate sources of open-source data (OSD), investigation of the dark web, and use of appropriate software, artificial intelligence (AI) and machine learning (ML).

OSINT is overt HUMINT as it is the people who create OSD and who possess OSD. Moreover, acquiring OSD and collating it into OSINFO for OSINT requires human effort. Due to ICT and IoT, OSINT can today give almost a 360-degree view of personalities, events, etc and so, is uniquely self-sufficient. Private commercial OSINT suppliers like BellingCat and Starlink, websites like https://liveuamap.com/, hobby OSINT providers like X (Twitter) handle of @OSINT_Insider and Telegram broadcasters like @DeepStateUA are blurring the lines of civilian efforts in war-fighting. This enhanced real-time public monitoring (सब कुछ सबको दिखता है) has imposed limitations on force manoeuvrability at strategic and operational levels. The so-called Wagner Group revolt against Russia in June 2023 is a case study of how a strategic manoeuvre to redeploy was supported by an elaborate Information Warfare (IW) plan of Prigozhin's coup against

President Putin. Thankfully, this BFT has also put caution into those wanting to conduct war crimes. It has also highlighted the criticality of faster OODA looping.

Military Lessons in OSINT

Internationally, the crowdsourcing exposes of Russian plans to invade Ukraine on February 24, 2019 using Google Maps, commercial satellite images, unencrypted telephone calls, Telegraph and Twitter has many lessons. The bombardment of pro-Russian Wagner Group's mercenaries in Popasna in August 2022 after the leak of a photograph of their location on a Telegram channel a few days earlier highlighted the outsourcing of detecting part of the kill chain.[9] This organised employment of citizens for OSINT by Ukraine is being called 'democratisation of the intelligence cycle'. The NATO IW attack on Russia over the alleged 'Bucha Massacre of 278 Ukrainians' in March 2022, exposed by OSINT and pursued by Human Rights Watch, has a different bag of lessons.[10] OSINT is definitely a double-edged sword.

India has witnessed both sides of this double-edged OSINT sword. Two important Indian OSINT successes: first, in 1984 Operation Meghdoot's pre-empting of Pakistani attempts to occupy Siachen Glacier based on OSINT of Pakistan buying special clothing from a foreign supplier.[11] Second, 2019 Indian decision to use the Indian Air Force for the surgical strike on February 26, 2019 (vis-à-vis use of the Indian Army for the Uri Surgical Strike of September 26, 2016). This may have been based on OSINT of Pakistani manoeuvres since December 2018 to force India to retaliate to the Pulwama Terror Attack with a land-based surgical strike. These manoeuvres were; the deployment of additional forces on the Line of Control (including Air Defence missiles),[12] the test fire of the LY 80 SAM missile on 11 January 2019[13] and nuclear missile tests from January 26 to 31, 2019 with IW message of "cold water over cold start strategy".[14] Pakistan's ultimate aim was to use this 'failure of

India's surgical strike' to influence the Indian General Elections 2024 using IW.[15] An interesting case of the same episode is that of Wing Commander Abhinandan's survival after his MiG-21 aircraft was shot down by Pakistan on February 27, 2019. He survived due to OSINT (or social media). And the behind-the-scenes story of his return by Pakistan, due to the Indian threats, admitted by Pakistani parliamentarians on October 29, 2020, became public knowledge 20 months later due to OSINT.[16] A possible example of Indian OSINT failure is Pakistan's Kargil Intrusions of November-December 1998 which remained hidden till May 3, 1999.

Thus today, OSINT is all pervading. It has roles in pre-war, war and post-war periods. It can provide: (1) situational awareness; (2) inputs on terrain, weather, technology and people; (3) threat/intent assessment; (4) inputs on targets; and (5) inputs on counter intelligence for automated intelligence preparation of the battlefield (IPB).[17] It is also necessary for projecting or exposing the lack of *jus ad bellum*, *jus in bello* and *jus post bellum*. OSINT serves the prosecution of war at the geo-strategic, strategic, operational and tactical levels. And, it is relevant in all types of conflicts/wars. It is the first step in the killing of a terrorist or an enemy soldier, and also in the killing of an opposing idea. The contribution of OSINT in the war effort will, however, vary with the level of penetration its drivers (ICT, IoT and smartphones) have in the objective area and among the target people.

Use of OSINT by India in War

About 2,300 years ago, Chanakya (or Kautilya) stressed on the use of intelligence in statecraft. Some quotes of his important advice are:[18]

- A king shall proceed to create spies: Spies under the guise of a fraudulent disciple, a recluse, a householder, a merchant, an ascetic practising austerity, a classmate or a colleague, a fire-brand, a poisoner, and a mendicant woman.

- Spies should be well-versed in inciting enemy forces to revolt, spreading false rumours about the enemy, mixing poison in the enemy's food supply, poisoning their drinking water, setting fire to the enemy's camp and bringing havoc and destruction, or if necessary, even assassinating the enemy leaders.
- If the end could be achieved by non-military methods, even by methods of intrigue, duplicity and fraud, I would not advocate an armed conflict.
- An arrow shot by an archer may or may not kill a single person; but skilful intrigue, devised by a wise man, may kill even those who are in the womb.
- The power of good counsel is superior to strength. Intelligence and science of politics are two eyes of the king to arrive at the best means and stratagem for a war.
- Conquest may be resisted at the slightest chance of a revolt within.
- Spies shall report on rumours circulating among people.
- The king shall protect his people from the intrigues of the enemy and win over/subvert people of the enemy country by gifts or sowing dissension.
- Power, place and time to launch a war are interdependent. If a king finds he is superior in all, he should proceed to crush the enemy.
- Clandestine agents shall wage psychological warfare against the enemy and weaken the enemy.
- Enemy shall be attacked when suffering from a calamity or when he is unprotected or when he is in unfavourable terrain.
- Chaos shall be created in the aggressor's camp and fort on the eve of an attack.
- The weak king shall arrange to kill the aggressor king.
- The enemy's army may be attacked in the rear and when it is staggering or has turned its back, attacked with the best of the forces.

- Soothsayers, readers of omens, astrologers, reciters of Puranas, intuitionists, and clandestine agents, those who helped the king perform the tricks and those who had witnessed them shall advertise them inside his territory. In the enemy's territory, they shall advertise, in particular.

If every social segment of the adversary's society using ICT, IoT and smartphones is penetrated, the quality of OSD inflow is likely to be high and good.

When we apply the rules of the OSINT Revolution (ICT, IoT and social media on smartphones) to this advice today, the OSINT game will undergo an indigenous metamorphosis. This new Chanakyan Model of OSINT, can be better than the ongoing NATO-Russia War in Ukraine and the Muslim-Jew Conflict in Israel. The Chanakyan Model is explained in the subsequent paragraphs.

Cultivating spies in every segment of adversarial society could be difficult, costly and time-consuming. However, if every social segment of the adversary's society using ICT, IoT and smartphones is penetrated, the quality of OSD inflow is likely to be high and good. Infiltration of made-in-China smartphones, laptops, and 5G technology into other countries is an appropriate example. This will help generate strategic intelligence i.e., political, economic, social and infrastructure intelligence.

Spies should spread rumours, incite revolt and create havoc in the enemy camp so that peace is won with lesser use of resources. A plan to achieve this requires a high level of BFT on the target society and people, including their vulnerabilities and motivations. OSINT can help construct the foundation of this plan, while HUMINT and TECHINT can help strengthen the foundation and build the superstructure.[19] After the attack, OSINT would again be the frontrunner in post-strike damage assessment (PSDA).

Achieving ends by non-military methods across the spectrum of conflict in offensive mode means destroying the ideology of the adversary and his/their will to fight. In defensive mode, it means protecting own ideology and will to fight. The key intelligence question for commanders wanting to use this strategy is: what is the opposing ideology, how much strength does the target society derive from it and is willing to suffer to defend it, and its strength—weakness—opportunity—threat (SWOT) analysis. The majority of information on this can be collated from OSINT i.e., newspapers, publications by think tanks, social media platforms, books, television, etc. HUMINT and TECHINT can then be used to corroborate OSINT and to provide an update on the latest situation. The selection of non-military means (various tools of IW) will be based on inputs of reconnaissance pull (RECONPUL) by a combination of OSINT, HUMINT and TECHINT. Technique/source of intelligence for PSDA would vary; OSINT biased in urban areas and TECHINT biased in rural areas. At the strategic level, PSDA should rely on OSINT and TECHINT, while at the tactical level, HUMINT and TECHINT could provide better inputs. This applies equally to military means for an attack on a platoon post to a major theatre offensive.

Skilful intrigue to kill even those who are in the womb requires a plan which will lead to the collapse of the adversary's societal beliefs resulting in long-lasting peace. RECONPUL for an intriguing entry into the adversary's 'womb' (centre of gravity) would require OSINFO on various parts of the adversarial system, its strengths to be avoided, and its weaknesses to be exploited. OSINFO by multiple sources, once collated and analysed, can then be corroborated by HUMINT and TECHINT. PSDA would be best if based on TECHINT and HUMINT, as measuring psychological damage to the 'womb' using OSINT could be difficult. For a kinetic attack on a physical 'womb', OSINT and TECHINT would be better able to provide BFT.

Good intelligence assessment to help arrive at the best strategy requires an effective intelligence cycle covering OSINT, TECHINT and HUMINT. OSINT collated over a period of time should form the bedrock of the intelligence assessment. It would include weather, terrain, an organisation for battle (ORBAT), effectiveness of weapons, morale of society, war readiness, war stamina, etc. Important assessment points of OSINT must be corroborated by TECHINT and HUMINT. This will help generate campaign intelligence i.e., geographic, terrain, religious, logistics and alliance intelligence.

Identifying favourable power, place and time to defeat the enemy is the most important and difficult set of intelligence questions. The required database on ORBAT, equipment, terrain and weather, state of the economy, and state of the society can be best collected by OSINT.

For conquest to be avoided due to the chance of a revolt within, the government has to secure its own population from subversion; especially in the launch pad of the offensive. This requires counter-espionage efforts whose foundation is OSINT.

To identify and neutralise the enemy's subversion of its own people and rumours being spread, the government has to rely more on HUMINT and TECHINT.

Identifying favourable power, place and time to defeat the enemy is the most important and difficult set of intelligence questions. The required database on ORBAT, equipment, terrain and weather, state of the economy, and state of the society can be best collected by OSINT. The final decision, however, may be based on corroboration by HUMINT and TECHINT. This will help generate tactical intelligence i.e., intelligence on weather, meteorology, obstacles, road networks and logistics systems.

Waging a psychological war to weaken the enemy requires drawing an IW strategy and plan(s) based on target audience analysis work (TAAW)

sheets. Most of the data required to fill TAAW sheets for each target audience comes from OSINT and TECHINT. For impact analysis (PSDA), however, IW staff will have to rely more on HUMINT and use social media as a link between intelligence, IW (strategic communication/ psychological warfare) and cyber warfare.

Attacking the enemy when weak or unprotected requires an assessment of the enemy's ORBAT and equipment, terrain, weather, society, economy and impact of a calamity. The majority of the inputs can be acquired through OSINT but, the final decision should be based on HUMINT and TECHINT. Pakistan's present case is an apt example. OSINT hints at Pakistan today being internationally isolated and its economy failing due to elite capture of resources, severe damage by floods of 2022, etc. This has to be corroborated by HUMINT and TECHINT to arrive at a correct strategy.

Weakening the enemy before an attack by an adverse internal situation requires a separate plan. The broad inputs for this plan can be provided by OSINT, but specifics will require HUMINT and TECHINT. The best D-Day and H-Hour will however be provided by HUMINT.

Killing the aggressor's leaders will require a mix of HUMINT and TECHINT, depending on the choice of weapons.

Attacking the enemy from the rear and exploiting fleeting opportunities requires BFT on the enemy's ORBAT, equipment, strategy, tactics, morale, and the impact of its own operations. The initial intelligence collection would be OSINT-biased. Thereafter, after the battle is joined TECHINT and HUMINT would be better able to provide inputs on PSDA to stay ahead in the OODA loop competition. In the non-kinetic sphere i.e., IW, OSINT would be better placed to give good assessments.

The use of agents to subvert and advertise PSDA as part of IW to weaken the enemy's resolve and to deny people's support should form part of the overall IW campaign (grey zone warfare). If done well, it

can end the war early and in a favourable post-war treaty. TAAW sheets for this part of the IW campaign will also draw heavily from OSINT. Thereafter, for impact analysis (PSDA), reliance will shift to HUMINT and TECHINT.

Conclusion

Technological advances in a globalised world have increased the quantity and quality of OSD available. OSINT has become the tool of first resort for IPB. The notion and rules of secrecy, surprise and deception have also changed dramatically. The involvement of tech-savvy citizens in the war effort is a new paradigm. Simultaneous use of smartphones for OSINT RECONPUL attacks and IW is making the cyberspace over the battle space more complex. The side with OSINT as a force multiplier will be able to alter military force disadvantage by leveraging OSINT. To win, our adversary has to disallow the exploitation of citizen soldiers for OSINT/IW and we must be able to freely use our own citizen soldiers for OSINT/IW like a well-oiled machine. Pakistan's Inter-Services Public Relations and Inter-Services Intelligence achieved this very well during the Pulwama-Balakot-Abhinandan-F16 episode in 2019. Lesson; India may need regulation so that the government's war-time monopoly over OSINT is ensured.

Recommendations. Our armed forces have to learn to secure our economy and national interests. Key recommendations on OSINT for the future Indian Military are given below.

- Invest in creating technological leadership educated in repeatedly winning day-to-day competitions, unlike the once-in-a-decade large-scale confrontation of the 20th century.[20]
- Recognise OSINT as a double-edged force multiplier and issue strategy and standard operating procedures (SOP) to exploit it. We also need a strategy and SOP to defend against OSINT, including its use for IW by our adversaries.

- Create awareness among all ranks and train intelligence careerists in the use of OSINT. This should include exploiting OSINT and defending against its exploitation by adversaries, and language, ICT and IoT skills.
- Include defence wings of embassies/high commissions across the world as the first line of real-time OSINT.
- Establish alliances for sharing of OSINT, with a focus on indigenous and in-house capabilities.
- Establish 24×7×365 OSINT monitoring centres at all levels. These must include disinformation (fact check) laboratories and have the capability to manage big data using AI and ML.
- Establish OSINT teams at all levels, with embedded civil subject matter experts. These must have inter-departmental OSINT sharing structures and protocols at each level. 'Eight Tribes Model' suggested by Amiy Krishna in his Field Marshal Manekshaw Essay 2020-21 for CLAWS is a good way ahead.[21] 'Tribes' refers to various government departments generating OSD and needing OSINT e.g., Ministry of Defence, Ministry of Home Affairs, Unique Identification Authority of India, State Police, Intelligence Bureau, Research and Analysis Wing, Media, academia and think tanks, and corporate business houses.
- Establish networks to share OSD and OSINT in real-time using Made-in-India applications, secure cellular networks and clean smartphones.
- Establish good OSINT collation systems for permanent institutional memory and better speed and accuracy of the competitive intelligence cycles and OODA loops.
- Restrict the use of ICT and IoT appliances in the military, both in peace and in war.

Notes

1. Libor Benes, "OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm." *Journal of Strategic Security,* No. 3 Suppl, 2013, pp. 22-37, at http://dx.doi.org/10.5038/1944-0472.6.3S.3
2. Peter Suciu, "Is Russia's Invasion of Ukraine The First Social Media War?," *Forbes*, 1 March 2022, at https://www.forbes.com/sites/petersuciu/2022/03/01/is-russias-invasion-of-ukraine-the-first-social-media-war/?sh=1301c75d1c5c
3 Cameron Colquhoun, "A Brief History of Open Source Intelligence." *BellingCat.* 14 July 2016, at https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/
4. TZ and Tamir Hayman, "Open-Source Intelligence and the War in Ukraine." *Institute of National Security Studies,* INSS Insight No. 1678, 5 January 2023, at https://www.inss.org.il/publication/russia-ukraine-intelligence/
5. Capt. Michael J Rasak, "Event Barraging and the Death of Tactical Level Open-Source Intelligence." *US Military Review*, January-February 2021, at https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Rasak-Open-Source-Intelligence-1.pdf?ver=OQwPyC0UYip2VkQsWIS7dQ%3D%3D
6. For this essay, other techniques of intelligence viz; imagery intelligence (IMINT) or measurement and signature intelligence (MASINT) are assumed to be part of either OSINT or TECHINT.
7. Tony H, "OSINT: The Powerhouse Behind Threat Intelligence and Counterintelligence—Uncovering Secrets." 7 March 2023, at https://www.linkedin.com/pulse/osint-powerhouse-behind-threat-intelligence-uncovering-tony-h
8. Heath Adams, YouTube Course "Open-Source Intelligence (OSINT) in 5 Hours." *TCM Security,* 11 January 2022, at https://www.youtube.com/watch?v=qwA6MmbeGNo
9. Matt Burges, "Their Photos Were Posted Online. Then They Were Bombed." *Wired*, 22 September 2022, at https://www.wired.co.uk/article/wagner-group-osint-russia-ukraine.
10. Human Rights Watch. "Ukraine: Russian Forces Trail of Death in Bucha." *HRW*, 22 April 2022, at https://www.hrw.org/news/2022/04/21/ukraine-russian-forces-trail-death-bucha
11. *The Economic Times*, "Siachen: All you should know about the world's costliest battlefield." 20 November 2019.
12. Major General Asif Ghafoor, Director General Inter Services Public Relations during press conference on 26 February 2019 admitted that Pakistan Army was ready for Indian ground surgical strike, but India decided to attack using the Indian Air Force, at https://www.youtube.com/watch?v=P6A9Jz5bEJE
13. *Dawn*, "Military test fires newly-inducted air defence weapon system", 11 January 2019, at https://www.dawn.com/news/1456708
14. RP Rajagopalan, "Pakistan's Nasr Missile: 'Cold Water' Over India's 'Cold Start'?", *The Diplomat* 31 January 2019, at https://thediplomat.com/2019/01/pakistans-nasr-missile-cold-water-over-indias-cold-start/

15. Prime Minister Narendra Modi to India TV on 5 May 2019; "Pakistan was expecting ground based surgical strike and was prepared for us. We decided to use Indian Air Force", at https://www.youtube.com/watch?v=hbY4HeZgNew. This OSINT bases analysis was provided by Defence Wing of High Commission of India in Islamabad on 18 February 2019.
16. See pinned thread on author's Twitter (X) account @LageRahoKashmir, at https://twitter.com/LageRahoKashmir/status/1457307591000821762
17. Zh Y Ju, Q Li, H Y Liu, X M Cui and Zh H Wang. "Study on application of open source intelligence from social media in the military." *Journal of Physics*, Conference Series 1507 (2020) 052017.
18. LN Rangarajan, *Kautilya: The Arthashastra* (New Delhi: Penguin Books India, 1992), pp. 151-220 and pp. 635-700.
19. US Army, Field Manual Interim No. 2-22.9, pp.2.2-2.9, December 2006.
20. Lt Col Akshat Upadhyay, "Amid Changing Nature and Character of War, the Need for Tech-Oriented Military Commanders for India." Observer Research Forum, 17 February 2023, at https://www.orfonline.org/research/amid-changing-nature-and-character-of-war/
21. Miya Krishna, "Institutionalising Open Source Intelligence in India: An Analysis." *CLAWS Manekshaw Paper*, 2020-21, at https://www.claws.in/static/REVISED-MP2021_AMIY-K_WINNER-1.pdf