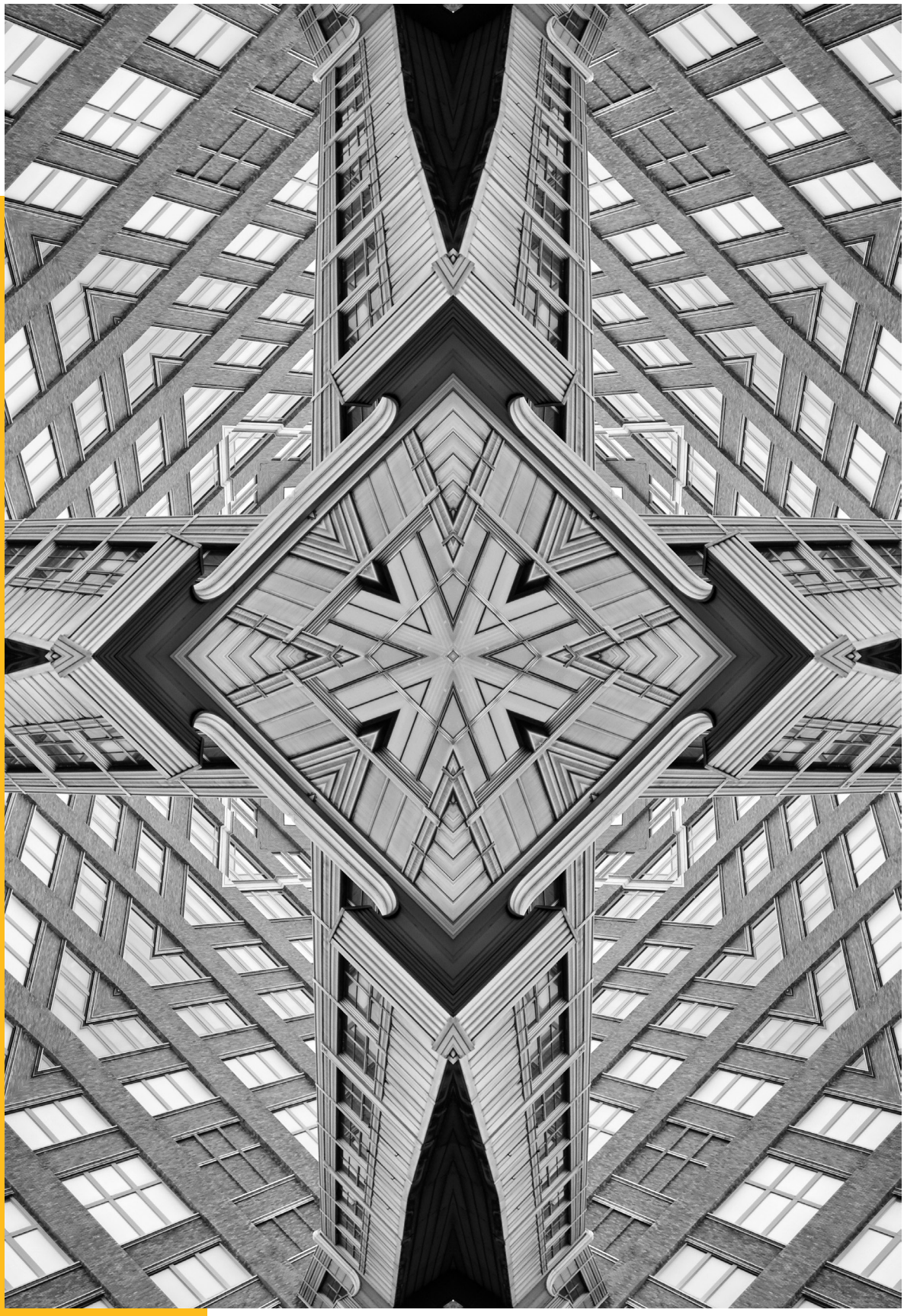
OBSERVER RESEARCH FOUNDATION

Occasional Paper



ISSUE NO. 555 JUNE 2026

Counter-OSINT and Its Implications for India's Security Strategy

Archishman Ray Goswami

Abstract

This paper examines the growth and implications of counter-open-source intelligence (OSINT) in the modern threat landscape. OSINT has traditionally seen limited use as a passive and often inviolable tool of validation under short-term tactical and operational horizons. Yet, in an accelerating, data-saturated, and volatile geostrategic terrain, the rise of counter-OSINT—the weaponisation of OSINT for deception and counter-espionage—renders such assumptions increasingly fallible. Today, social-media-fuelled disinformation and other forms of synthetically generated content have flooded open-source platforms, enabling threat actors to not just corrupt the tools and methods principally employed in OSINT work, but also corrode the decision dominance enjoyed and deployed by an adversary based on its existing intelligence capacities. The paper concludes with some recommendations for India's national security community on how to tackle counter-OSINT across different levels of strategic and military doctrine.

Attribution: Archishman Ray Goswami, "Counter-OSINT and Its Implications for India's Security Strategy," *ORF Occasional Paper No. 555*, Observer Research Foundation, June 2026.

Introduction

The global threat landscape is nebulous and incendiary, defined by the confluent effects of multipolarity and a proliferation of sophisticated, off-the-shelf technologies resulting from rapid commercialisation. Intelligence capacities infuse and bind these disparate features, underpinned by growing global consensus on the importance of accelerated intelligence data fusion, to equip deploying states with the necessary informational advantage or 'decision dominance' as per their strategic requirements. This pursuit of speed and synthesis sets the backdrop for the cut-throat geopolitics of 2026. Most importantly, it draws attention to open-source intelligence (OSINT) and its corollary, the subject of this paper: counter-OSINT.

OSINT is hardly a new arm of intelligence. Agencies have held and utilised records of publicly available information, including newspaper clippings, academic papers, radio broadcasts, and other journalistic sources, since the American Civil War (1861–65) and the two World Wars.[1] However, the key methods and mediums that it relied upon have now changed. Modern OSINT, while continuing to draw insights from traditional research and media, increasingly deals in near real-time (NRT)[a] with vast, proliferating digital and commercial data streams, and is often pursued by autonomous or non-state actors, including private investigative firms, journalists, and even amateurs.[2] Moreover, while there is an extensive body of research on OSINT and its place within the strategic intelligence ecosystem, its double-edged use in counter-espionage and deception—counter-OSINT—is less well-documented, a gap this paper seeks to fill.

This paper explores the implications of counter-OSINT as a distinct form of modern counter-intelligence for India's national security, contextualising its analysis through the race for accelerated intelligence fusion that defines global security today. It starts by defining what counter-OSINT means and where its varied derivatives sit within international security, alongside associated utilities and risks. Sections two and three analyse the consequences of using counter-OSINT in military affairs and higher-level policymaking, respectively. Section four discusses global examples relating to the professionalisation and institutionalisation of counter-OSINT within national security architectures, before concluding with a set of recommendations for India to consider.

a The near-instantaneous exchange of data and directives between sensors and intelligence consumers/command centres, driven by technological advancement.

Defining OSINT and Counter-OSINT

This study will use the following definition of OSINT: "Intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[3]

Despite its history (it comprised approximately 80 percent of all Western intelligence products at the end of the Cold War in the late 1980s), OSINT's credentials as a 'collection discipline' have been much debated.[4] In today's data-infused world, these bona fides are generally conceded, with Western intelligence services collecting around 90 percent of their raw product through public digital platforms, including social media from the late 2010s.[5] In some respects, it has even come to subsume other collection disciplines, with scholars such as Stephen Mercado noting that imagery intelligence (IMINT) today "is becoming such a commercial commodity as to be in danger … of ceasing to be an 'INT'" or a distinct variety of intelligence collection. Commercial satellite imagery providers such as Maxar Technologies (now Vantor), Google Earth, and ICEYE lead transformation in this space through the commercialisation of geospatial imagery across open-source digital platforms.[6] OSINT has also introduced new possibilities—and hindrances—for human intelligence (HUMINT), allowing case officers to develop a target's character profile prior to recruitment by scouring the candidate's 'digital dust' on social media and other sources, using technologies like artificial intelligence (AI).[7] Likewise, open-source flight-path data may provide insights to intelligence officials tracking a target's movements. Journalists and amateur investigators have started using open-source flight data in their work, from tracking Libyan warlord Khalifa Haftar's flights to Elon Musk's private jet. [8,9]

Advances in internet traffic analysis have cemented OSINT's importance and position as a form of intelligence activity. While the collection of secret information for what scholars such as Jennifer Sims have called "decision advantage" or "the capacity for rapid action" remains central, filtering signals from the increasingly enormous quantities of noise across public commercial or digital platforms is equally important for today's spies.[10] The challenge for them is akin to 'drinking from a fire hydrant,' compounded by OSINT's manipulation for purposes of strategic deception.

Defining OSINT and Counter-OSINT

Over much of its history, OSINT has been seen as the most 'authentic' and trustworthy form of intelligence, as, unlike other 'INTs,' it is gleaned from public sources and therefore more likely to be genuine. However, it is also fallible, given factors such as the advent and growing ubiquity of sophisticated technologies, such as AI and the NRT transmission of information, disinformation, and opinion through social media, which can be further manipulated in an audiovisual-centric broadcast landscape through deepfake imagery. Today's intelligence services must thus contend with the rise of counter-OSINT or "adversarial OSINT:" *The intentional manipulation of OSINT by threat actors to undermine an adversary's decision and strategic advantage, pursued as an active tool of counter-espionage and deception rather than as a passive tool of intelligence collection and data harvesting that OSINT tends to be used for*.[11]

Counter-OSINT too has a storied history. During the Second World War, British Security Coordination (BSC), a covert propaganda unit of Britain's Security Intelligence Service (SIS), was briefly tasked with spreading disinformation or 'black propaganda' against the Nazis within the American press, with the intention of drawing the United States (US) into the Allied War effort prior to its official entry in 1941, and subsequently to keep up the momentum of public support for the war effort.[12] The British also ran the Information Research Department (IRD) from 1948 to 1977, a covert information warfare bureau within Britain's Foreign Office tasked with disseminating 'white' (factually correct), 'black' (disinformation), and 'grey' (a mixture of the two) anti-Communist propaganda.[13] Today, similar counter-OSINT disinformation occurs at a larger scale, mostly through digital means. Social media and abundant digital data enable malign actors to curate algorithm-driven information warfare to target individuals and groups with increasing effectiveness and granularity. In 2025, the Trump administration tried to force Chinese internet technology firm ByteDance to sell its social media company TikTok's US operations to a consortium of American investors, mainly to gain control over TikTok's algorithm, which Washington described as a national security risk. But ByteDance (and, by extension, Beijing) retained the operations.[14] This dispute brought to light the evolving character of digitally enhanced disinformation, alongside the geopolitical competition over its most mundane open-source building blocks.

Modern counter-OSINT also takes different forms. Technology enables threat actors to weaponise the tools and methods OSINT investigators rely upon to infer meaning from raw data. OSINT employs certain tested methods like geolocation,[b] search engine "dorking,"[c] and other forms of metadata analysis.[d,15,16,17] These techniques have proved to be the most reliable means of authenticating provenance and sifting truth from falsehood within data harvested from the public internet. Data scientist and scholar Amelia Acker even argued, as late as 2019, that a close reading of metadata by discerning analysts "will often reveal intentions, slippages, and noise, which can further reveal automated manipulation," particularly in the context of counter-disinformation.[18]

However, today, metadata itself is easier to falsify, presenting a challenge to validation processes within intelligence architectures. Technological advancement and growing access to miniaturised, cheaper commercial technologies now enables a wider array of actors to doctor metadata and deceive target states in the open-source intelligence sphere. In the past, OSINT platforms such as the Wireless Geographic Logging Engine (WiGLE) used data produced by WiFi stumblers to make public information to image and geolocate wireless networks in different vicinities, metadata analysis of which could allow OSINT investigators to track individuals through connected devices, such as smartphones and computers.[19] Likewise, fitness platforms like Strava allow users to publicly share 'heatmaps' of their movements with other users, which allowed investigators to track US forces in secret bases or camps in sensitive locations like Afghanistan, Syria, and Djibouti,[20] and more recently, to identify French warships *en route* to the Middle East.[21] Commercial location data has also been used by Iran in the ongoing war in the Gulf to triangulate the position of US forces and strike them.[22]

Today, global positioning system (GPS) spoofing allows national intelligence services to doctor metadata itself, providing false OSINT and geolocation data. Both sides in the Russia–Ukraine war have leveraged GPS spoofing, falsifying smartphone data to deceive weapons systems, particularly drones/loitering munitions that rely on synthesised intelligence

b The extraction of actionable insights from publicly available data to ascertain the geographical location of individuals, entities, or events.

c Advanced search techniques used on search engines to find specific and often hidden information on the public internet by exploiting loopholes and coding configurations.

d The process of uncovering and examining the hidden data embedded within digital files such as creation dates, access history, and user activity.

provided by multiple sources, including OSINT.[23] As this technology improves, so will open-source metadata's capacity for quicker and more sophisticated deception. Precedents have already been established within the civil aviation sector, where GPS or Automatic Dependent Surveillance-Broadcast (ADS-B) data—information that allows for flight tracking on open-source platforms like FlightRadar and is often used by global air traffic control to prevent air accidents—has been deliberately falsified.[24] This was observed in late 2025 when GPS spoofing affected numerous flights at Delhi's Indira Gandhi Airport. While the risks of this activity are well established, it also indicates new challenges for OSINT-driven geolocation.[25] Metadata, once the most authentic means of corroborating OSINT data, is now increasingly susceptible to deceptive fabrication through falsified information on platforms like WiGLE or Strava, or ADS-B data tampering.

Results obtained through search-engine dorking are similarly susceptible to malicious falsification using generative and agentic AI by threat actors to conjure false account sheets, identity documents, audio-visual content, and more. Beginning in the early 2020s, threat actors worldwide have been recorded using generative AI to forge authentic-looking documents, from cyber-criminals luring victims with AI-generated bank account sheets,[26] to North Korean spies fabricating real military IDs in their shadow war with South Korea.[27] In modern counter-intelligence, generative AI could be used by nation-states to leave a trail of deliberately deceptive 'public' information and evidence for the 'other side' using dorking. The same applies to social media intelligence (SOCMINT), a subcategory of OSINT, pursued through methods like dorking.[28] Here, AI technologies could be used to fabricate and plant seemingly authentic evidence to supplement the 'legends' used by HUMINT officers, adding credibility to their backstories.[29] This was seen in 2022, in the case of Sergey Chekasov alias 'Viktor Muller Ferreira,' a Russian intelligence operative tasked with infiltrating the International Criminal Court in the Hague, where seemingly authentic evidence of an active digital profile was curated by his handlers to allay suspicions of adversary counter-intelligence investigators and provide credence to the backstory crafted for him.[30] These tactics can even be deployed at larger levels to 'astroturf' or "coordinate deceptive and spontaneous information campaigns in order to influence public opinion" in an adversary's society

Defining OSINT and Counter-OSINT

"by imitating the grassroots activity of autonomous individuals" on open-source platforms such as Telegram.[31] One need only look at recent cases of weaponised AI-enhanced social media profiles, such as 'Sophia Naga', a false social media profile created by Pakistan's Inter-Services Intelligence (ISI) in the mid-to-late 2010s to exploit and fabricate grievances in India's Northeast and revive dormant Naga separatism.[32] As commercial AI evolves to provide increasingly sophisticated fabrications of documentary evidence, as seen with Google's Nano Banana Pro that provides uncannily 'real' photographic imagery, the authenticity of OSINT methodologies like dorking may be undercut.[33]

With the rise of full-spectrum conflict, counter-OSINT will require national intelligence and counter-intelligence services to recalibrate current strategies with a greater emphasis on speed to achieve first-mover advantages within rapidly changing narrative and epistemic gaps. This will help distil signals from the noise of unstructured jumbled disinformation and filter credible/relevant OSINT in cyberspace. It demands the employment of new technologies to speed up validation under all-source assessment, the integration of flexible forms of cooperation with diverse entities within the strategic communications space, and the integration of advanced digital forensic systems at all levels of the intelligence cycle at both the strategic and tactical levels.

Counter-OSINT and Current Intelligence: Implications for Policy

Wider discourses around the role of intelligence in international politics often overlook the critical utility provided by intelligence analysis, which determines the larger intelligence and national security strategy (NSS) informing a state's pursuit of national interest. This general rule of thumb places a premium on the importance on the objectivity of intelligence analysis, at least in an idealised sense. In the words of Sherman Kent, the chief of the CIA's Office of National Estimates in the 1950s and '60s and the widely regarded 'father of intelligence analysis,' it is better "to be a bookie," numerically grading estimates and the likelihood of certain events on a cold, detached basis, "than [to be] a goddamn poet."[34]

The primary challenge counter-OSINT poses for intelligence analysis is, therefore, its corrosion/weaponisation of objectivity, particularly at the higher echelons of national net assessment. As OSINT proliferates across digital platforms, opportunities abound for threat actors seeking to leverage the combined effects of growing demand for, and time pressures on, the delivery of intelligence to policy customers. The challenge is particularly acute in 'current' intelligence analysis, defined by the United Kingdom (UK) government as "intelligence that reflects the present situation at strategic, operational and/or tactical levels … generally reflecting a moment in time and remaining perishable."[35] Current intelligence analysis occurs under extremely short time frames, often being generated within minutes by analysts to provide the first reading of an incident, soon after occurrence, to policymakers. Consequently, current intelligence analyses rely primarily on OSINT, given that classified intelligence tends to take longer to source, vet, and integrate into a preliminary diagnosis. In contrast, OSINT can be rapidly harvested using automated agents such as AI and large language models (LLMs), and cross-referenced across seemingly 'validated' sources.

The circumstances under which current intelligence analysis occurs, coupled with its resultant overreliance on OSINT data, creates strategic vulnerabilities. Under such time pressures, scholars like Philip Davies (2024) note that the "limited shelf-life" of current intelligence and the "frenetic pace" demanded of its analysts by policymakers "do not permit analytic tradecraft to be applied," because of which current intelligence

analysis, more often than not, relies "more on informed intuition than structured or rigorous methods" generally applied elsewhere.[36] Such circumstances cause three main problems.

First, analysts choose to rely predominantly on OSINT in their readings on current intelligence, both because of the relative ease of sourcing under time pressures, and because it is seen as publicly validated and most likely to be genuine. Yet, as proven, while OSINT is still a valued collection discipline, it is equally (if not more) susceptible to fabrication as any other source. That OSINT is not a "controlled source" unlike others, where "the intelligence function can vouch for or has detailed insight into the origin and handling of the information," only aggravates analytical difficulties, with Davies noting additionally that "the webpage, Telegram channel or other social media identity" that OSINT investigators and intelligence analysts rely on "are often far more opaque in provenance while also embodying the same risks of hostile control" as any other 'covert' form of counter-espionage, "whether direct or indirect, conscious or unconscious."[37] Therefore, OSINT's first-mover advantage equally generates opportunities for actors using counter-OSINT to reach the other side's policymakers at the earliest stage of any development. Deceptive information carried through OSINT platforms is likely to reach a policymaker before any other data.

Second (and relatedly) is the problem of bias and flawed cognition. Current intelligence, as the first piece of intelligence a policymaker usually receives, is prone to cultivate an 'anchoring bias'[e] in their mind.[38] Counter-OSINT can aggravate such existing biases within higher-level strategic planning by undermining the information fidelity of current intelligence. An anchoring bias produced by intentionally deceptive counter-OSINT, which current intelligence assessment rapidly incorporates, can damage subsequent decision-making, even if truthful intelligence is provided later. Knowledge of this feature of current intelligence analysis can help attackers leverage their capacities to manipulate adversary responses. Under such

e "A cognitive bias that causes us to rely heavily on the first piece of information we are given about a topic," often at the expense of later inputs.

conditions, an attacker armed with sophisticated AI infrastructure to facilitate methods such as 'sentiment analysis'[f] can tap into the dominant biases of both analysts and policymakers by planting intelligence on open-source platforms that is most quickly accessible to or likely to appeal to them. This may be based on prior intelligence gathered on the analysts' strategic priorities, domestic political compulsions, or cultural nuances. When baked into current intelligence analysis, the costs of such deception can be heightened due to the ensuing 'anchoring bias', undermining even genuine later intelligence inputs.[39] This was observed in August–September 2022, when Ukraine's armed forces deceived Russian forces via OSINT during the Kherson and Kharkiv campaigns respectively, using a sentiment-analysis-enhanced disinformation campaign titled 'Kherson First' that was meant to tap into pre-existing Russian biases around Ukrainian military objectives. This allowed Kiev to maintain the element of surprise by keeping the Kremlin's military elite off-track in their response to the counterattack.[40] Applied to the bureaucratic politics of national intelligence estimation and strategic planning, such precedents underscore the potential for exploitation of OSINT's existing dominance within current intelligence analysis, and its prominent role in shaping policymaking from the outset.

The third problem emerges in relation to OSINT-driven intelligence liaison and strategic intelligence disclosure (SID), where an adversary's deceptive counter-OSINT can damage global standing or trust among liaison partners using OSINT for strategic signalling. The absence of 'disclosure dilemmas'—where the hazards of publicising or exchanging intelligence with partner(s) are compounded by the risks it poses to methods and agents/means of collection—make OSINT vital to both modern intelligence liaison and to SID. Evidence of this would be China's real-time sharing of commercial satellite imagery with Iran during Operation Epic Fury,[41] and with Western intelligence agencies publicising OSINT data during amid the war in Ukraine (2022–present) as part of their strategic communications.[42] Yet, these dependencies only deepen the damage effective counter-OSINT can cause for an adversary. Disinformation, the falsification of metadata, and other means of counter-OSINT, for instance, can embed false data for a state to unintentionally disclose through its

f The process of analysing large volumes of text or data to determine whether it expresses a positive, negative, or neutral sentiment.

SID, undermining its strategic communications and causing reputational damage, similar to what the US intelligence community suffered in 2003 after its public disclosure of incorrect 'slam dunk' evidence that Saddam Hussein's regime in Iraq possessed nuclear weapons.[43] Likewise, the exchange of intelligence based on falsified OSINT data can damage trust among partners.

The strength of a national counter-intelligence service lies in its reputation as a trustworthy partner to allies with whom it trades intelligence and often forms the basis for diplomatic activity. The geopolitical and reputational costs of counter-intelligence failure can have negative ripple effects on the intelligence it procures from other states. Perhaps nowhere was the scale and impact of this cost more visible than during the Cambridge Spy Scandal of the 1960s, when the defections of several high-ranking British intelligence officials to Moscow hampered intelligence liaison with the US under the 'Special Relationship.' This led to Washington demanding that London "clean house regardless of whom may be hurt," if it wanted intelligence liaison to continue unhindered, the incident having "severely shaken the State Department's confidence in the integrity of officials of the Foreign Office."[44] Counter-intelligence risks to intelligence liaison and the credibility of SID in the modern age may hinge on the speed and effectiveness with which a national agency responds to counter-OSINT. This involves the pre-emptive detection of deceptive OSINT before it corrupts the processes intelligence exchanged with international partners.

Counter-OSINT and the Military: Tactics and Strategy

As with higher-level strategy, military operations and tactics are also vulnerable to the use of counter-OSINT, which is becoming central to strategic and tactical battlefield considerations. Modern military planning relies on automated 'observation, orientation, decision, action' (OODA) loops and AI-driven 'kill chains' to quite an extent, accommodative of inputs from OSINT, and commercial data (particularly with respect to satellite imagery and topographic information) to provide greater situational awareness at the 'observation' stage.[45] Countries like the US have been known to use their extensive and sophisticated digital intelligence processing software for mainly OSINT data such as social media traffic and commercial satellite imagery in their implementation of command, control, communications, intelligence, surveillance, target acquisition, and reconnaissance (C3ISTAR).[46] The XVIII Airborne Corps of the US Army is said to have relied on these OSINT-dense information flows to craft intelligence recommendations and target patterns for Ukrainian strikes on Russian barracks in Mariivka in the early hours of New Year's Day 2023, and prior to that, in its attempted assassination of Valery Gerasimov, Russia's chief of general staff, in May 2022.[47] The intelligence-centric processes of C3ISTAR and geolocation in both cases were primarily fed by OSINT, particularly the close monitoring of Russian military social media feeds on public social media platforms alongside commercial geospatial intelligence (GEOINT) collection on the targeted regions.[48] Similarly, the Intelligence Division of the Israel Defence Forces (IDF) has made extensive use of their 'Gospel' AI system, which synthesises sensor data from multiple sources with inputs gathered through OSINT to conduct targeted attacks in Gaza, and more recently, Iran.[49]

Such changes have aided the development of an increasingly seamless interface between private-sector OSINT collectors and military end-users. OSINT-driven C3ISTAR has been sustained by Palantir's Project Maven, the US Department of War's initiative to embed AI and machine learning into warfighting systems.[50] Ukraine itself has recalibrated liaison between private organisations focused on OSINT collection and analysis and its own armed forces. Investigative firms such as Molfar have used their expertise in OSINT collection and analysis to gather information on the movements of key Russian troop detachments using publicly available

social media data traffic, passing on this actionable intelligence to the Ukrainian armed forces for targeting.[51] Separately, the proliferation of OSINT in contemporary asymmetric conflicts also enables conventionally weaker parties to acquire decision advantage for leverage. This has been evidenced by Hamas's use of both traditional media and digital open-source material terror attacks against Israel since as early as the 1990s.[52]

The main challenge here, as noted previously, is tactical; relating to the unique high-pressure situations under which commanders must respond as per available intelligence. Given such circumstances, and the varied forms of physical attack that comprise the experience of battle, tactical intelligence must be immediately actionable and ironclad in terms of trust. Yet, a well-placed piece of deceptive OSINT relating to the topographic features of a point of attack beyond visible horizons is possible through the falsification of commercial satellite imagery, GPS spoofing of apparent adversary positions, and other forms of metadata tampering. When applied *en masse* to 'flood the zone' with disinformation, these can cause significant military damage. In particular, it can amplify the 'latency problem'[g] that most AI agents, including Enterprise AI and intelligence analysis systems, contend with.[53] Accordingly, even if the AI agent is able to synthesise the most appropriate intelligence assessment for its users by cross-referencing the falsified metadata with previous validated information entered by commanders, the extension of the 'lag time' or latency as it 'thinks' its way through to an actionable input can leave the consumer or the field vulnerable to enemy attack or deception. The high pressure and threat of physical danger that shapes cognition in battle only augments these challenges.

Such obstacles are particularly concerning for special operations forces (SOF), for whom intelligence received and acted upon must be geographically bound and time sensitive.[54] Indeed, modern SOF doctrines increasingly accommodate OSINT scraping into day-to-day operational planning, as seen in the Find, Fix, Finish, Exploit, Analyse, Exploit, Disseminate (F3EAD) process.[55] Within this process cycle, intelligence must be shared in NRT under conditions of political sensitivity without any

g The lag time between inputting data and receiving actionable inputs in relation to prompts or human demands.

compromise in methods and means of collection. In this, OSINT activity is seen to be a critical part of the 'find,' 'fix,' and occasionally 'exploit' phases. In such high-risk high-pay-off missions, the stakes and possible costs of deceptive counter-OSINT are far greater and latency problems and deception caused by counter-OSINT can provide atomised levels of threat.

Counter-OSINT can also confuse an adversary's autonomous targeting systems, such as loitering munitions, particularly when they rely on such data to identify and neutralise targets independently of human command. In July 2021, Iran allegedly used its Shahed-136 drone to conduct a fatal kamikaze attack on the Israeli-owned merchant vessel, the *MV Mercer Street* in the Gulf of Oman, with the drone's internal software generating the plan of attack independently on the basis of transponder data about the ship—information that was publicly accessible online through commercial platforms,[56] or could have been generated through a simple dorking exercise. The incident also draws attention to the potential risks of using such intelligence. Had the transponder data been doctored, for instance through deepfake imagery of measurements and signals intelligence (MASINT) graphical data, and subsequently made available through commercial platforms, the drone, engineered to act independently of human guidance, could well have missed its intended target or even attacked a different vessel to cause Iran diplomatic embarrassment. This vulnerability adds the possibility of friendly fire on one's own forces or on allies. Counter-OSINT, therefore, reinforces the need for armed forces worldwide to accelerated efforts towards faster, triangulated, and more resilient systems of validation.

Using and Institutionalising Counter-OSINT: Global Examples

Keeping in mind the above analysis, can—and should—governments formalise counter-OSINT, just as they have other collection disciplines? While few global examples of formal and separate national OSINT agencies exist, examining what fledgling attempts have been made can help gauge whether such a goal is possible, or even desirable.

Counter-OSINT has shown the greatest promise for formalisation within the realm of counter-disinformation. In the West, the growing security challenges posed by state-sponsored information/cognitive warfare has catalysed the establishment of counter-disinformation agencies and doctrines. In 2022, Sweden established a 'Psychological Defence Agency' to defend itself against perceived threats from Russian disinformation.[57] Finland has expanded and modernised its whole-of-society approach to national security, called Sisu, to meet the new challenges of social-media-driven disinformation and its proliferation in the form of deepfakes and doctored audiovisual data.[58]

Elsewhere, OSINT and counter-OSINT have been incorporated under existing subdivisions of intelligence agencies. The US's primary OSINT organisation, Open Source Enterprise, operates under the Central Intelligence Agency's (CIA) Directorate of Digital Innovation, adopting a mostly passive view of OSINT collection, as opposed to the active character of counter-OSINT.[59] Washington's other 'intelligence' organisations, including the State Department's in-house all-source intelligence assessment agency, the Bureau of Intelligence and Research (INR), also rely primarily on OSINT, although here, too, their responsibility remains limited to passive analysis rather than the pursuit of counter-espionage and deception/counter-deception.[60] In the UK, the 'National Centre for Geospatial Intelligence' (NCGI), a smaller bureau within Defence Intelligence (DI), is tasked with serving as the UK's "national lead for geospatial intelligence" and as "the defence lead for OSINT," focused on gathering and analysing commercial satellite imagery.[61]

Russian and Chinese models provide more in terms of leveraging OSINT for counter-espionage and deception against adversaries. Beijing is known to rely mainly on 'private' commercial actors for its OSINT requirements.[62] These third- and fourth-party commercial actors' networks provide

niche skills and expertise to the People's Liberation Army (PLA), thereby serving several targeted strategic purposes. One such contractor, DataExa, operates the "Tianji Intelligence Information Centre Platform," an OSINT platform that uses technologies such as deep and machine learning, alongside automated web crawlers, to harvest enormous quantities of open-source data for the PLA to exploit, fabricate, and disseminate against adversaries, all the while ensuring plausible deniability for the Chinese state.[63] Indeed, evidence shows that the use of automated web crawlers by Chinese commercial OSINT firms has been used to doctor such metadata as AdSense Revenue Per Mille (RPM)[h] that OSINT investigators often rely on, indicating the number of 'hits' a website receives.[64] By using web crawlers to generate 'artificial hits,' Chinese commercial actors can actively falsify such data. Equally, such private actors also enable China's information warfare campaigns with tools of counter-OSINT, using sentiment analysis algorithms to measure global perceptions of China and craft narrative campaigns accordingly.[65]

Russian approaches similarly prioritise plausible deniability in counter-OSINT operations. Companies such as Lavina Pulse and its subsidiary, 'Avalanche,' have been targeted by US sanctions due to their alleged counter-OSINT operations on behalf of the Kremlin and its allies, allegedly using vast digital infrastructures of automated web crawlers and chatbots to amplify and de-amplify content on social media and facilitate other forms of strategic deception against domestic and international opponents in digital spaces.[66] The growth of such companies points towards a shift in the Russian approach. Russian counter-OSINT is shifting away from the centralised model of direction illustrated by organisations such as the Wagner Group's erstwhile Internet Research Agency, which, despite making efforts, failed to conceal the Kremlin's sponsorship of its information warfare operations. Today, there's a stronger preference for the decentralised, hub-and-spoke system offered by private companies like Avalanche.

Both models offer different counter-OSINT approaches. The Western model is vertical, subordinating OSINT and counter-OSINT to existing national intelligence agencies, yet seeing the collection discipline mainly

h A unit of measurement to estimate the earnings made per every thousand 'clicks' on a webpage.

Using and Institutionalising Counter-OSINT: Global Examples

as a corollary to standard and passive intelligence analysis and assessment. Disinformation and counter-disinformation appear to be the only domains where the kinetic character of counter-OSINT is fully accounted for, with defences constructed to meet the strain it applies on national resilience in its fluid and evolving form. On the other hand, the Chinese and the Russians have adopted a horizontal model, one where plausible deniability and active counter-espionage/deception is emphasised, and direct state involvement concealed through the subsidiary actions of 'private' entities. Lessons from both models can shape how India might govern, pursue, and defend against counter-OSINT going forward.

Counter-OSINT's Implications for India

The analysis presented above underscores the implications of counter-OSINT for both defenders and attackers in modern conflicts and geopolitics. As India reorients its intelligence strategy in the mid-2020s to meet its new status as the world's fourth-largest economy and, according to the Lowy Institute Asia Power Index, Asia's third-largest power, it will need to account more closely for the role of counter-OSINT in national security.[67]

The first question is whether India requires a separate and formal counter-OSINT agency. While the Indian state must establish both defensive/offensive counter-OSINT capacities, both for its own security and to pursue its interests more vigorously in a dangerous global order, the risks of establishing a separate and public agency for this purpose, even to a limited end such as counter-disinformation, are high. Domestic politicisation, partisanship, and malicious speculation over the agency's true intent can further degrade the information landscape to which such an agency would need to respond. The precedent established by foreign adversaries' exploitation of domestic partisan discourse around India's recent military conflicts with Pakistan further highlights the potential associated risks.[68]

A two-pronged approach might be a solution. The first prong would be the formation of a smaller, initially clandestine organisation operating under existing bodies like the National Security Council Secretariat (NSCS) and tasked with securing national intelligence analysis and assessment against corruption by deceptive open-source data. This agency would serve as a second line of defence against adversarial counter-OSINT, integrating advanced digital forensics and quantum technology to validate the possibilities of metadata falsification and fabricated audiovisual content disseminated on open-source platforms like social media. The first line of defence would involve a network of private actors, emulating the Chinese model. Operating through a hub-and-spoke model, these organisations would ideally specialise in key sub-domains of counter-OSINT, from instantaneous open-source data harvesting through automated web crawlers to counter-information warfare through traditional and non-traditional news media.

Counter-OSINT's Implications for India

Indian intelligence will equally need to establish secure and rapid channels for all-source intelligence fusion and net assessment. While OSINT will remain important, its corroboration against information gathered from other secret collection disciplines, particularly HUMINT, at increasingly short notice and with a view towards speed, is essential. The challenges will likely persist and even be exacerbated in both battlefield scenarios and strategic planning at higher levels of government. With the former, one may only look to the EagleEye headset developed by Anduril Industries, an AI-powered Augmented Reality/Virtual Reality headset for troops that fuses together commercial satellite imagery with topographic information and heat-mapping to give its wearer a more transparent view of the immediate battlefield environment.[69] In the future, the customised NRT tactical intelligence fusion and analysis that such technology could provide to its military user could equally encompass OSINT data inputs, which may or may not be deceptive.

As similar forms of military technology enabling greater battlefield transparency make their way into India's military arsenal, military intelligence agencies, including the Defence Intelligence Agency and the individual intelligence organisations of the tri-services, face a clear counter-OSINT challenge: that of enabling rapid, even customisable intelligence synthesis and imaging for individual soldiers, which is able to incorporate OSINT inputs while filtering out deceptive information quickly and within high-pressure battlefield settings in NRT. On the other hand, the advantages of existing technology for an attacker can be immense. Deceptive OSINT inputs, for instance through AI-generated commercial satellite imagery, can be strategically 'placed' to make their way into an EagleEye-like headset of an enemy soldier, and subsequently determine targeting patterns against them.

Such problems will need to be overcome through efforts to rapidly incorporate validated HUMINT data into NRT current intelligence analysis and assessment. The challenge of sourcing and translating raw HUMINT inputs at short notice during crises has long hindered holistic intelligence analysis, resulting in an overreliance on OSINT. While all-source assessment and inter-agency intelligence sharing is baked into the functioning of India's intelligence apparatus through platforms such as

the Multi-Agency Centre (MAC), the challenge will be to devise ways to synthesise and cross-reference multi-source intelligence inputs, including validated HUMINT, on which a premium should be placed, with greater speed and in digestible formats for diverse consumers. Indeed, distilling HUMINT's complexity into readily available data points/inputs that are readily translatable into current intelligence analysis is the need of the hour. Although there have been recent improvements to the MAC in terms of intelligence fusion, real-time mapping, and satellite imaging, these advances will need to be built upon to meet the unique requirements of a fast-paced intelligence landscape facing the compounded challenge of adversarial counter-OSINT.[70]

Such changes are only possible if Indian intelligence agencies expand their pool of reliable HUMINT data to validate OSINT in real time. As with Western agencies, the explosion of public information on public digital platforms has also reflected in intelligence collection by Indian agencies, with over 90 percent of it estimated to come from technological intelligence (TECHINT), the bulk of which is OSINT.[71] Indian police forces and intelligence agencies are also liaising more closely with private firms in fields such as data analytics, with an emphasis on harvesting/analysing OSINT data gathered from the surface, dark, and deep webs, to predict and counter criminal behaviour and national security threats. Ahmedabad Police's use of 'Prophecy Alethia,' a predictive policing model generated by Delhi startup Innefu Labs, and its OSINT suite Innsight, is an example.[72] This overdependence, however, presents a vulnerability for intelligence analysis, leaving agencies exposed to fabricated or deceptive OSINT data with insufficient HUMINT data to corroborate it.

Going forward, the challenge will be to find ways to access and corroborate HUMINT data at short notice and in real time, across a variety of analytical platforms, to produce credible intelligence assessment for policymakers. An emphasis on AI-enabled data fusion and the construction of channels to bring raw HUMINT into closer and faster dialogue with data harvested from open-source platforms will be critical for Indian intelligence agencies. All-source assessment centred on rapidly synthesised HUMINT data by India's intelligence agencies will only grow in terms of importance. Balancing the need for human intuition and analytical rigour with the

demand for speed in high-pressure environments to reduce overreliance on any single collection discipline and the natural openings for deception that it is accompanied by, will be a key challenge.

Such efforts, when coupled with active red-teaming in peacetime/wartime to test the strength of one's analytical resilience in the face of counter-OSINT cognitive threats, can be crucial to ensure the veracity of intelligence delivered to policymakers. For these to happen, India's intelligence agencies will need to overhaul existing recruitment practices to incentivise young and technically proficient professionals to support counter-OSINT measures. To this end, India may invest in whole-of-society efforts towards national defence and resilience against information warfare, like Finland, both with a view towards securing the nation against an adversary's counter-OSINT and to cultivate a generation of technically proficient young professionals capable of leading and running India's future counter-intelligence against adversary counter-OSINT.[73]

None of this portends a perceived decline in OSINT's utility for intelligence analysis. However, effective counter-OSINT will require Indian intelligence agencies to integrate advanced digital forensics tools into the platforms and systems from which raw data is extracted for processing. The use of Electronic Network Frequency Analysis (ENFA), for instance, may enable India's intelligence agencies to limit difficulties caused by metadata falsification. ENFA is a forensic analysis tool that requires the use of highly advanced technologies identifying unique signature patterns within audiovisual content otherwise undiscernible to the human ear, or alternative detection platforms.[74] This information, once gleaned from close observation of lighting patterns and mains hum, enables investigators to geolocate locations via the nearest power grid operating at the detected frequency, or detect tampering, without having to rely on metadata. As more audiovisual content saturates the internet, accelerated by social media, these methods must become central to intelligence analysis, with greater focus placed on their integration within point-of-capture devices.

Moreover, this focus on integrating advanced forensic technologies into platforms such as the MAC and point-of-capture devices to rapidly validate material gathered using OSINT will require close technological

Counter-OSINT's Implications for India

collaboration between India's intelligence community and the private sector. Digital forensics and the development of technologies to validate imagery and audiovisual content at the point of capture and on handheld devices such as smartphones, now increasingly comprise a new frontier for deep-tech exploration. Indeed, their commercial utility has been most salient in newsroom settings, with companies such as London-based start-up OpenOrigins using blockchain cryptography to help secure archival footage for broadcast agencies like the UK's ITN, against AI content.[75] The importance of incorporating such technologies into national security and intelligence work is vital. At a time when over 50 percent of surface web content is estimated to be AI-generated, a discerning intelligence analyst armed with advanced forensics technology software systems such as these (ideally sourced indigenously), and embedded either within handheld devices like smartphones or higher-order intelligence infrastructure such as spy satellites, could be well-placed to sift credible signals within open-source data from synthetically generated AI/deepfake 'noise.'[76]

Similarly, offensive operations using AI can be used to pursue kinetic counter-espionage across open-source platforms against malign actors. Such forms of counter-OSINT might involve the use of software such as 'Nightshade,' a 'data poisoning' tool currently used in creative industries to prevent the unauthorised use of artwork, which adds false pixel-specific imagery or data into AI companies' LLM training systems.[77] In the hands of national intelligence agencies, these may be used both as a first line of offence and defence to undercut malign actors' use of deception on open-source digital platforms.

Conclusion

This paper underlined the importance of taking greater cognisance of OSINT's active and kinetic role as a means of counter-espionage, as opposed to the passive and verificatory role it is perceived as playing within national decision-making. It built upon this analysis to make a case for faster all-source/net assessment and intelligence fusion in an accelerating technological and geopolitical landscape. After establishing what counter-OSINT is and the mutative forms its digital avatars can take, it examined implications of its use by threat actors at two levels: first, in current intelligence analysis within higher-level policy, and second, in military strategy. It then discussed efforts being made in the collective West, and in Russia and China, to professionalise counter-OSINT as part of their respective approaches to national security and power projection. Finally, it welded together the evidence presented in the preceding sections to discuss how India may use counter-OSINT to secure its interests in a dangerous new world order.

This paper also raised new questions about the future of counter-OSINT. In analysing the use of ENFA as a more effective device of counter-OSINT, able to bypass the risks of falsified metadata, it implied the need to develop new technologies and strategies to defend against or take advantage of these evolved forms of counter-espionage across open-source platforms. The trends it discussed also point to the need for closer public–private partnership in this space, as evidenced from its assessment of the role played by digital forensics companies like OpenOrigins in providing defenders faced against a fluid and rapidly changing threat picture with some degree of advantage.

Translating these imperatives into policy and execution will be vital for national intelligence agencies going forward. As states vie for technological dominance, those that are able to not just defend but leverage the offensive potential of counter-OSINT will be the primary intelligence powers of the future. India must seize the initiative before it is too late—or risk being left behind.ORF

Archishman Ray Goswami *is Non-Resident Associate Fellow at Observer Research Foundation's Strategic Studies Programme and a DPhil (International Relations) candidate at the University of Oxford.*

Endnotes

1 Ludo Block, "The Long History of OSINT", *Journal of Intelligence History,* 23, no. 2 (2024): 99.

2 James P. Marshall, "Near-Real-Time Intelligence on the Tactical Battlefield The Requirement for a Combat Information System" (Maxwell Air Force Base: Air University Press, 1994), https://apps.dtic.mil/sti/tr/pdf/ADA290065.pdf.

3 Bowman Miller, "Open Source Intelligence (OSINT): An Oxymoron?" *International Journal of Intelligence and Counterintelligence,* 31, no. 4 (2018): 706.

4 Peter Gill and Mark Phythian, *Intelligence in an Insecure World,* (Cambridge: Polity Press, 2018).

5 Gill and Phythian, *Intelligence in an Insecure World*.

6 Stephen Mercado, "A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age," in *Secret Intelligence: A Reader,* eds. Christopher Andrew, Richard Aldrich, Wesley Wark (Abingdon: Routledge, 2009), 80.

7 Liam Walsh, "AI and the Changing Art of Human Intelligence Tradecraft", Center for International Security and Economic Strategy, November 21, 2025, https://www.linkedin.com/pulse/ai-changing-art-human-intelligence-tradecraft-cises-uk-7dpxe/.

8 "Libya: Haftar Plane 'Lands in Israel' for a Two-Hour Visit," *Middle East Eye,* January 15, 2022 https://www.middleeasteye.net/news/libya-haftar-plane-lands-israel-two-hour-visit.

9 Jason Koebler, "Emails Show SpaceX Bungled Elon Musk's Private Jet Privacy", *Vice News,* May 24, 2023, https://www.vice.com/en/article/emails-show-spacex-bungled-elon-musks-private-jet-privacy/.

10 Jennifer Sims, *Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar*, (Oxford: Oxford University Press, 2022): 7.

11 "Adversarial Tactics for Shaping OSINT," Fivecast, June 2, 2023 https://www.fivecast.com/blog/adversarial-tactics-for-shaping-osint/.

12 William Boyd, "The Secret Persuaders," *The Guardian,* August 19, 2006, https://www.theguardian.com/uk/2006/aug/19/military.secondworldwar.

13 Hugh Wilford, "The Information Research Department: Britain's Secret Cold War Weapon Revealed," *Review of International Studies*, 24 no 3 (1998): 353–369.

14 Bobby Allyn, "TikTok Signs Deal to Give U.S. Operations to Oracle-led Investor Group," *NPR,* December 18, 2025 https://www.npr.org/2025/12/18/nx-s1-5648844/tiktok-deal-oracle-trump.

15 "OSINT Sources – Using Geolocation for OSINT Investigations," Neotas, https://www.neotas.com/osint-sources-geolocation-osint/.

Endnotes

16 Esteban Borges, "Google Dorks: Top Tips and Tricks for Advanced Search Intelligence," Recorded Future, May 26, 2024, https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks.

17 Neeraja Hariharasubramanian, "Metadata Analysis Explained: Meaning, Methods, and Cyber Forensics Use," Fidelis Security, January 30, 2025, https://fidelissecurity.com/cybersecurity-101/network-security/metadata-analysis/.

18 "Reading Metadata to Combat Disinformation and Fake News Campaigns," The University of Texas at Austin School of Information, January 22, 2019, https://ischool.utexas.edu/news/reading-metadata-combat-disinformation-and-fake-news-campaigns.

19 Wigle.net, https://wigle.net/.

20 Alex Hern, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases," *The Guardian,* January 28, 2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

21 Sofia Ferreira Santos, "Officer Reportedly Leaks Location of French Aircraft Carrier with Strava Run," BBC, March 20, 2026, https://www.bbc.co.uk/news/articles/cd9vdel17wqo.

22 Raphael Satter, "Exclusive: US Military Personnel Are Being Targeted Using Location Data, Pentagon Letter Shows," Reuters, May 28, 2026, https://www.reuters.com/business/media-telecom/pentagon-says-us-military-personnel-are-reportedly-being-targeted-using-location-2026-05-28/.

23 Kateryna Hodurova, "Ukrainian GPS Spoofing for Repelling Drone Attacks could Indirectly Affect Smartphone Clocks, General Staff Says," *The Kyiv Independent,* November 5, 2024, https://kyivindependent.com/ukrainian-electronic-warfare-could-indirectly-affect-smartphone-clock-while-repelling-drone-attacks-general-staff-says/.

24 Jeremy Bennington, "How GPS Spoofing Impacts Automatic Dependent Surveillance-Broadcast Systems," *Spirent,* March 10, 2025, https://www.spirent.com/blogs/how-gps-spoofing-impacts-automatic-dependent-surveillance-broadcast-systems.

25 Saurabh Sinha, "Explained: What is GPS Spoofing and How It Disrupted Delhi Flights," *Times of India,* December 2, 2025, https://timesofindia.indiatimes.com/city/delhi/explained-what-is-gps-spoofing-and-how-it-disrupted-delhi-flights/articleshow/125121593.cms

26 Satish Lalchand et al., "Generative AI Is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking," Deloitte, May 29, 2024, https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html.

27 Jane Lanhee Lee, "North Korean Hackers Used ChatGPT to Help Forge Deepfake ID," *Fortune*, September 14, 2025, https://fortune.com/2025/09/14/north-korean-hackers-openai-chatgpt-deepfake-id-south-korea-military/.

Endnotes

28 David Gioe, "'The More Things Change': HUMINT in the Cyber Age," in *The Palgrave Handbook of Security, Risk, and Intelligence*, eds. Robert Dover, Huw Dylan, Michael S. Goodman (London: Palgrave Macmillan, 2017), 215.

29 Gioe, "'The More Things Change': HUMINT in the Cyber Age."

30 Gordon Corera, "Russian GRU Spy Tried to Infiltrate International Criminal Court," *BBC,* June 16, 2022, https://www.bbc.com/news/world-europe-61831961.

31 Rosanna De Rosa and Annarita Criscitiello, "Framing Disinformation and Malign Foreign Information Influence: A Focus on the Electoral Arena," *Media, War, and Conflict* (2025): 13, https://doi.org/10.1177/17506352251345666

32 Rujuta Thete, "Accounts Run From Pakistan Share Viral Posts Against India, Defend Nagaland," *The Quint*, April 25, 2025, https://www.thequint.com/news/webqoof/nagaland-woman-tortured-kidnapped-video-goes-viral-fact-check#read-more.

33 Ruben Circelli, "ChatGPT's Latest AI Image Generator Is Its Best Yet, But Nano Banana Pro Is Still Better," *PCMag*, December 28, 2025, https://www.pcmag.com/news/chatgpts-latest-ai-image-generator-is-its-best-yet-but-nano-banana-pro.

34 J. Peter Scoblic, "Beacon and Warning: Sherman Kent, Scientific Hubris, and the CIA's Office of National Estimates," *Texas National Security Review* 1, no. 4 (2018): 112, https://tnsr.org/2018/08/beacon-and-warning-sherman-kent-scientific-hubris-and-the-cias-office-of-national-estimates/.

35 Development, Concepts and Doctrine Centre (DCDC), *Joint Doctrine Publication 2-00: Intelligence, Counterintelligence and Security Support to Joint Operations*, 4th ed. (Shrivenham, UK: DCDC, 2023), 30, https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.

36 Philip H. J. Davies, "The Defence Intelligence 'Daily Update': Current Intelligence as Public Service Announcement," in *Intelligence and Contemporary Conflict: Communication in Diplomacy, Statecraft, and War*, ed. Matthew Hefler (Stockholm: Bokförlaget Stolpe, 2024), 164.

37 Davies, "The Defence Intelligence 'Daily Update,'" 168.

38 "Why Do We Compare Everything to the First Piece of Information We Received?" *The Decision Lab*, https://thedecisionlab.com/biases/anchoring-bias

39 "What Is Sentiment Analysis?" IBM, https://www.ibm.com/think/topics/sentiment-analysis.

40 William Mitchell, "Assessing Deception Projection via OSINT: The Case of the Ukraine 2022 Counter-Offensive," *The Journal of Applied Operational Intelligence* 1, no. 1 (2024): 41–62.

Endnotes

41 Henry Zwartz, "Chinese AI Satellite Intelligence Helping Iran Target US Forces with 'Incredible Precision,' Analysts Say," *ABC News*, April 6, 2026, https://www.abc.net.au/news/2026-04-06/chinese-satellite-intelligence-helping-iran-target-us-forces/106535420.

42 Shaun Walker, "A War Foretold: How the CIA and MI6 Got Hold of Putin's Ukraine Plans and Why Nobody Believed Them," *The Guardian*, February 20, 2026, https://www.theguardian.com/world/ng-interactive/2026/feb/20/a-war-foretold-cia-mi6-putin-ukraine-plans-russia.

43 Paul Pillar, "Intelligence, Policy, and the War in Iraq," *Foreign Affairs* 85, no. 2 (2006): 15–27.

44 SpyScape, "The Cambridge Spy Scandal That Haunts Britain," https://spyscape.com/article/the-cambridge-spy-scandal-that-haunts-britain.

45 Col. Shane Hamilton and Lt. Col. Michael Kreuzer, "The Big Data Imperative: Air Force Intelligence for the Information Age," *Air and Space Power Journal* 32, no. 1 (2018): 7, https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-30_Issue-2/2018_2_11_hamilton_s_eng.pdf.

46 Tate Nurkin et al., "China's Advanced Weapons Systems," *Jane's by IHS Markit*, May 12, 2018, 16, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf.

47 Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," *Journal of Global Security Studies* 9, no. 2 (2024): 12.

48 King, "Digital Targeting."

49 Harry Davies, Bethan McKernan, and Dan Sabbagh, "'The Gospel': How Israel Uses AI to Select Bombing Targets in Gaza," *The Guardian*, December 1, 2023, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.

50 Pranoy Jainendran, "AI in Real-Time Warfare: Lessons from Project Maven," ORF, December 30, 2025 https://www.orfonline.org/expert-speak/ai-in-real-time-warfare-lessons-from-project-maven.

51 "Ukrainian Company Uses Social Media, Open Source Technology to Counter Russian Invasion," *PBS*, April 19, 2023, https://www.pbs.org/newshour/show/ukrainian-company-uses-social-media-open-source-technology-to-counter-russian-invasion.

52 Netanel Flamer, "'The Enemy Teaches Us How to Operate': Palestinian Hamas Use of Open Source Intelligence (OSINT) in Its Intelligence Warfare Against Israel (1987–2012)," *Intelligence and National Security* 38, no. 7 (2023): 1171–1188.

Endnotes

53 Andrew Marshall, "Why Latency Is Quietly Breaking Enterprise AI at Scale," *The New Stack*, August 6, 2025, https://thenewstack.io/why-latency-is-quietly-breaking-enterprise-ai-at-scale/

54 *Janes*, "Use of OSINT to Support Special Operations Forces," *The World of Intelligence*, podcast audio, December 16, 2022, https://open.spotify.com/episode/19k9qi6LExRFHGwUn5Xffb?si=4b0f9fab08834330.

55 Gabriel Fanelli, "F3EAD: SOF Specific Targeting in the Intelligence Cycle," *SOF Support*, December 23, 2025, https://sofsupport.org/f3ead-sof-specific-targeting-in-the-intelligence-cycle/.

56 OCIMF, "Loitering Munition – The Threat to Merchant Ships," August 2023, 11, https://www.maritimeglobalsecurity.org/media/db1onvme/loitering-munitions-the-threat-to-merchant-ships.pdf.

57 "Our Mission", Psychological Defence Agency, https://mpf.se/psychological-defence-agency/about-us/our-mission.

58 James Brooks, "Finland's Battle Against Fake News Starts in Preschool Classrooms," *ABC News*, January 5, 2026, https://abcnews.go.com/International/wireStory/finlands-battle-fake-news-starts-preschool-classrooms-128902330.

59 Steven Aftergood, "Open Source Center (OSC) Becomes Open Source Enterprise (OSE)," *Federation of American Scientists*, October 28, 2015, https://fas.org/publication/osc-ose/.

60 US Department of State, "Open Source Intelligence Strategy," Bureau of Intelligence and Research, May 2024, https://2021-2025.state.gov/wp-content/uploads/2024/05/INR-Open-Source-Intelligence-Strategy.pdf

61 "National Centre for Geospatial Intelligence (NCGI)," GOV.UK https://www.gov.uk/government/groups/national-centre-for-geospatial-intelligence-ncgi.

62 Philip Ingram, "Inside China's Hidden OSINT Networks Shaping the Future of Intelligence Warfare," *Karve*, April 29, 2025, https://www.karveinternational.com/insights/inside-chinas-hidden-osint-networks.

63 Insikt Group, "Private Eyes: China's Embrace of Open-Source Military Intelligence," *Recorded Futures*, June 1, 2023, https://assets.recordedfuture.com/insikt-report-pdfs/2023/ta-2023-0601.pdf.

64 Andrew Nguyen, "Chinese and Brazilian AI Bots Are Crawling Websites and Killing AdSense RPM," *ClashPanda*, October 26, 2025, https://clashpanda.com/chinese-and-brazilian-ai-bots-are-crawling-websites-and-killing-adsense-rpm/.

65 Ingram, "Inside China's Hidden OSINT Networks Shaping the Future of Intelligence Warfare."

Endnotes

66 Thomas Brewster, "Exclusive: Meet Russia's Cambridge Analytica, Run by a Former KGB Agent Turned YouTube Influencer," *Forbes*, March 21, 2023, https://www.forbes.com/sites/thomasbrewster/2023/03/21/andrei-masalovich-avalanche-russia-cambridge-analytica/?sh=23b713c6424a.

67 "India Reaches 'Major Power' Status on Asia Power Index, Ranks 3rd After US and China," *Economic Times*, November 28, 2025, https://economictimes.indiatimes.com/news/india/india-reaches-major-power-status-on-asia-power-index-ranks-3rd-after-us-and-china/articleshow/125633652.cms?from=mdr.

68 "India's Opposition Demands Proof of Surgical Strikes," *Dawn*, October 5, 2016, https://www.dawn.com/news/1288108.

69 Anduril Industries "EagleEye: Superpowers for Superheroes," YouTube, October 16, 2025, https://www.youtube.com/watch?v=x9B02pFKpJo.

70 Arun Dhital, "India's AI-Powered Intelligence Grid: Amit Shah Inaugurates New Multi Agency Centre at North Block in New Delhi," *Swarajya*, May 17, 2025, https://swarajyamag.com/news-brief/indias-ai-powered-intelligence-grid-amit-shah-inaugurates-new-multi-agency-centre-at-north-block-in-new-delhi.

71 Neeraj Chauhan, "India's Agencies Increasingly Depend on Tech Intel," *Hindustan Times*, January 9, 2021, https://www.hindustantimes.com/india-news/indias-agencies-increasingly-depend-on-tech-intel-101610160966455.html.

72 "MHA Commends Innefu Labs' AI Systems in Ahmedabad Safe City," *Indian Television*, November 25, 2025, https://www.indiantelevision.com/mam/digital/mha-commends-innefu-labs%E2%80%99-ai-systems-in-ahmedabad-safe-city-251125.

73 Shona Murray, "Finland Adopts an All-Society Model to Build National Defence," *Euronews*, July 10, 2025, https://www.euronews.com/my-europe/2025/10/07/finland-adopts-an-all-society-model-to-build-national-defence.

74 "Electric Network Frequency (ENF) Signals: The Hidden Fingerprint in Every Recording," *Strike Labs*, https://www.strikelabs.io/compulsions/electric-network-frequency-enf-signals-revolutionizing-media-authentication.

75 "ITN Partners with OpenOrigins to Safeguard its Historic Archive from AI Threats," ITN, June 4, 2024, https://www.itn.co.uk/media-centre/itn-partners-openorigins-safeguard-its-historic-archive-ai-threats.

76 Frank Landymore, "Over 50 Percent of the Internet Is Now AI Slop, New Data Finds," *Futurism*, October 14, 2025, https://futurism.com/artificial-intelligence/over-50-percent-internet-ai-slop.

77 Victoria Masterson, "What is Nightshade – the New Tool Allowing Artists to 'Poison' AI Models?" World Economic Forum, November 14, 2023, https://www.weforum.org/stories/2023/11/nightshade-generative-ai-poison/.

Images used in this paper are from Getty Images/Busà Photography (cover and page 2) and Getty Images/Otto Stadler (back page).

OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org