Joshi, Manoj

**Book**

# Open-Source Intelligence has arrived

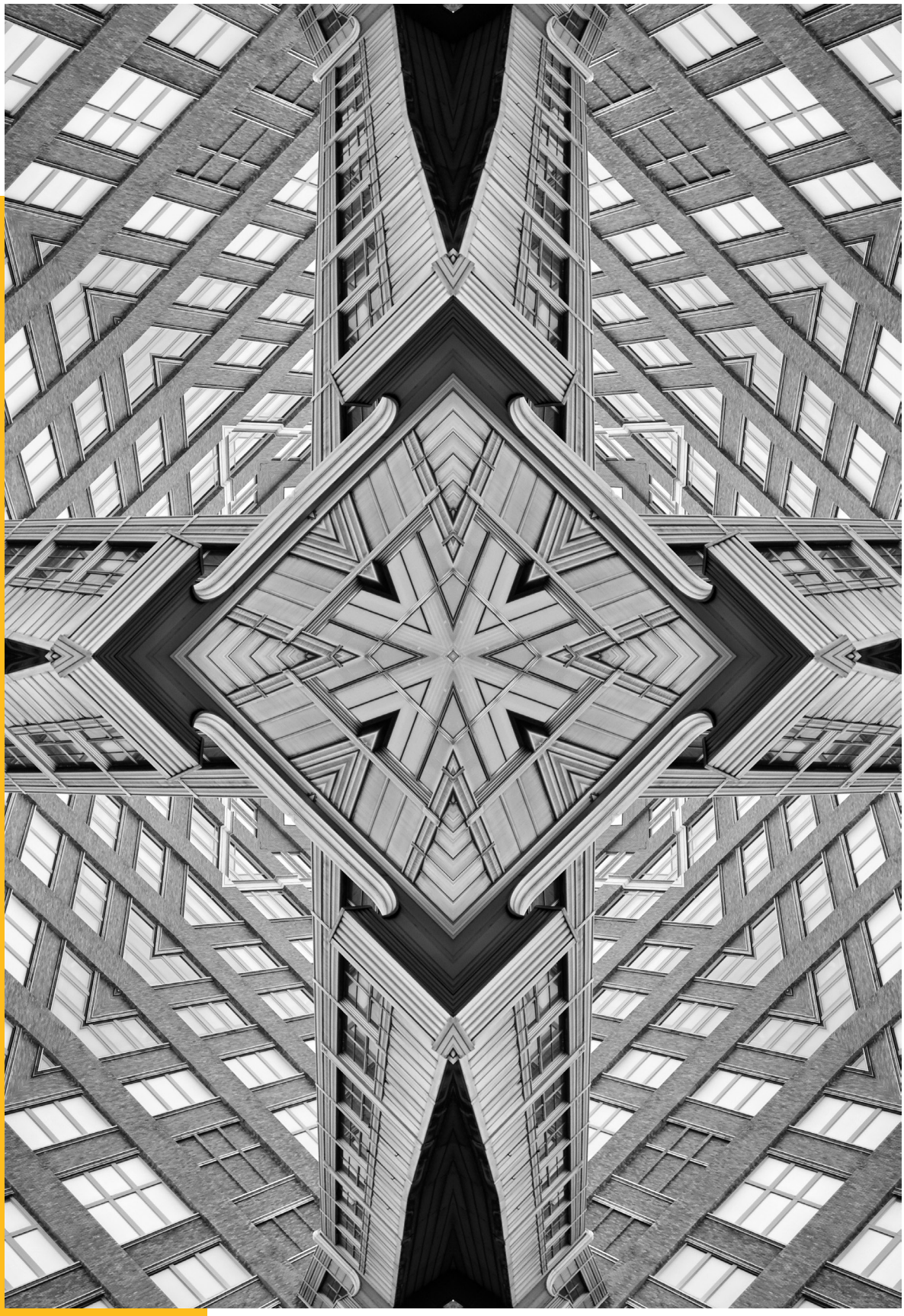
**Provided in Cooperation with:**
Observer Research Foundation (ORF), New Delhi

*Reference:* Joshi, Manoj (2023). Open-Source Intelligence has arrived. New Delhi, India : ORF, Observer Research Foundation. https://www.orfonline.org/wp-content/uploads/2023/10/ORF_OccasionalPaper_415_Open-SourceIntelligence.pdf.

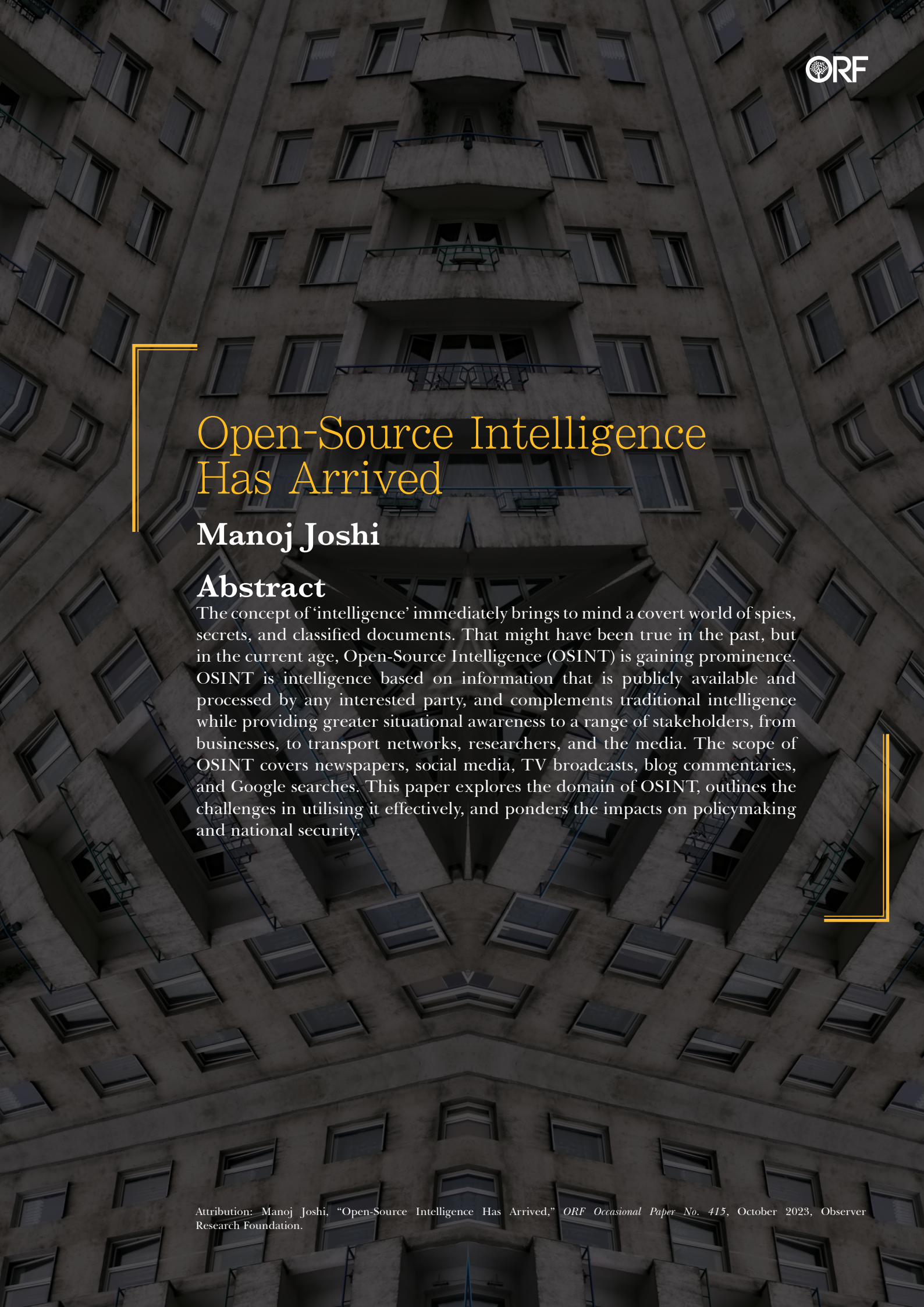
This Version is available at:
http://hdl.handle.net/11159/654413

OBSERVER RESEARCH FOUNDATION

# Occasional Paper



ISSUE NO. 415 OCTOBER 2023



# Open-Source Intelligence Has Arrived

**Manoj Joshi**

## Abstract

The concept of 'intelligence' immediately brings to mind a covert world of spies, secrets, and classified documents. That might have been true in the past, but in the current age, Open-Source Intelligence (OSINT) is gaining prominence. OSINT is intelligence based on information that is publicly available and processed by any interested party, and complements traditional intelligence while providing greater situational awareness to a range of stakeholders, from businesses, to transport networks, researchers, and the media. The scope of OSINT covers newspapers, social media, TV broadcasts, blog commentaries, and Google searches. This paper explores the domain of OSINT, outlines the challenges in utilising it effectively, and ponders the impacts on policymaking and national security.

Attribution: Manoj Joshi, "Open-Source Intelligence Has Arrived," *ORF Occasional Paper No. 415*, October 2023, Observer Research Foundation.

# Introduction

The classic definition of 'intelligence' is "the discovery of secrets by secret means" and its goal is to provide foreknowledge of the world to policymakers.[1] Open-Source Intelligence (OSINT), meanwhile, connotes using all available public sources of information for national security purposes, business intelligence, research, maintaining law and order, and media reportage.[a]

OSINT has emerged in the past two decades as a powerful tool that can be used for a variety of purposes. It is becoming increasingly important as the amount of publicly available information continues to grow exponentially. A 2018 study by American think tank, RAND, has cited a document issued by the Office of the Director of National Intelligence in 2011 defining OSINT as "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."[2] The same study noted that the rise of the Internet and social media platforms has led to complications introduced by new sources and methods that include "online expression of personal sentiment, photographs of local places and happenings, and publicized social and professional networks." Computers and data analysis techniques have enhanced a user's capability to process this information and "find implications that are of intelligence value."[3]

Indeed, the growth of the internet has led to a connectivity revolution and a veritable explosion of accessible information. Today, any commentator, political leader, academic, NGO, or think tank analyst who have access to the internet can share information that is potentially useful for their own goals. Likewise, there is a growing cadre of amateur analysts and hobbyists using a variety of software and artificial intelligence (AI) translation tools to analyse information for a range of everyday purposes.

a Publicly available sources can include newspapers, magazines, court documents, TV, radio, internet, video, geospatial data, photos, commercial satellite imagery—indeed, all publicly available data. The information being sought can be anything from names and positions of company employees, to subdomain information and web server versions in use; everything is fair game.

# Introduction

OSINT relies on hobbyists, gifted amateurs, researchers, and analysts in startups and companies focusing on software, data collection, analysis and dissemination. This is facilitated by a parallel "space revolution" where private players own hundreds of satellites that generate imagery that is free, or available at a price and can be accessed in real time and on-demand. The advent of nano Cube Satellites[b] which can be used for earth observation and amateur radio, has democratised satellite ownership. Aided by advances in automated analysis and machine learning, satellites and other technological aids help convert data to actionable intelligence which can be used by governments, business enterprises, media organisations and other stakeholders for various purposes.

As American academic Amy Zegart has pointed out, "Intelligence is a sense making enterprise" used by policymakers to "understand the past and anticipate the future."[4] OSINT is able to provide a far more dynamic and faster understanding of the world and is unparalleled in its speed and efficacy. Most intelligence agencies rely on OSINT in some way, and for the US Department of Homeland Security, it serves as a first line of intelligence.[5]

In its essence, OSINT is different from traditional intelligence, primarily on the issue of sources and their reliability. Nevertheless, OSINT has manifest advantages that cannot now be ignored by traditional intelligence officials. The sheer volume of information that is available, and the existence of "hobbyists" and non-government talent that is willingly processing it, could be a boon to governments. Yet this can be so only if they are willing to recognise that they cannot cope with the information revolution on their own, and if they can develop effective partnerships with the non-government sectors to utilise the vast ocean of information for intelligence purposes.

OSINT works at two levels. First, by analysing commercial satellite imagery, automatically translated foreign newspapers, magazines and social media, and all publicly available data, it provides quick in-depth information to opinion-makers, thereby affecting political discourse. In the case of India and China, for example, since the governments provided few details of what was happening in Galwan in 2020, if at all, most details were from analyses of commercially available satellite imagery and other material disseminated through social media.

b These satellites are just about 10x10x10 cm, weighing 2 kg.

At the second level, OSINT has been a tool of the government—a function that goes back to the Second World War and the founding of agencies like the US's Foreign Broadcast Monitoring Service (FBMS) and the United Kingdom's (UK) BBC Monitoring whose job at that time was to record, translate, transcribe and analyse shortwave broadcasts of the Axis powers.

Chinese intelligence agencies, too, are investing in OSINT to learn about the capabilities of the US military in the Pacific and beyond. An analysis by Recorded Future, an American private company dealing with OSINT, has detailed China's efforts to collect public data from the Pentagon, think tanks, and companies dealing with military periodicals like Jane's, Don, ProQuest and Ebsco.[6]

At the same time, China has moved to curb access to its largest academic database, China National Knowledge Infrastructure (CNKI), as of April this year. This privately owned database contains government reports, academic journals, dissertations and papers published in China since 1915 in a range of areas relating to politics, technology and economy. This had been accessible throughout the world, but now will be limited to Chinese institutions.[7]

To be sure, intelligence agencies do not simply collect information for its sake, but do so specific to the needs of policymakers, such as a National Security Adviser tasked to negotiate on the Sino-Indian border or a foreign minister raising a sensitive issue with their foreign counterpart. Intelligence is not merely providing the information but offering insights, too— the motivations, goals and tactics of an adversary negotiator, or the timing and direction of an infiltrating covert operative or militant.

The traditional intelligence community uses a variety of technological tools to do their task; they also find it useful to exploit human frailties such as greed for money, sex, or desire for revenge. In terms of providing a larger awareness in today's world, however, OSINT is vital for its unparalleled speed and efficacy. Analysts therefore need to effectively mix OSINT with classified information to obtain valuable insights.[8]

All the traditional areas of intelligence are well-funded and understood. There is need now to comprehend and promote the use of OSINT.

# U.S. Intel: A Brief History

The Foreign Broadcast Monitoring Service, launched in 1941, changed its name to Foreign Broadcast Intelligence Service (FBIS) shortly after the Japanese army attacked the US naval base at Pearl Harbor in Hawaii in December of that year. After the war it became the Foreign Broadcast Information Service under the control of the new Central Intelligence Agency. Over time, like BBC Monitoring, it was tasked to cover all foreign mass media, radio, TV and print. BBC Monitoring has, however, remained an arm of BBC World Service and provides services to the rest of BBC and the UK government.[9]

The US Army created its own Asian Studies Detachment in 1947 which was part of the US intelligence setup in Japan. Japanese personnel with expertise in various languages[c] served as linguists, collectors, analysts, translators and librarians. They published a daily Force Protection and Situational Awareness Report (FPSAR) which was also posted in the FBIS website.[10]

Under the CIA's Directorate of Science and Technology, the FBIS monitored and translated media sources from around the world using 20 monitoring stations and their reports were circulated within the governmental system and could be read in a US government press office. This could typically include translations of All India Radio broadcasts from cities like Patna, Bhubaneswar and Chennai, duly transcribed, translated and printed. An associated outfit called the Joint Publications Research Service (JPRS) provided translations of content from foreign print media. This material were used along with data from US Government-sponsored R&D by the National Technical Information Service (NTIS) of the US Department of Commerce, tasked with collecting and organising foreign scientific, technical, engineering, and business information.[11]

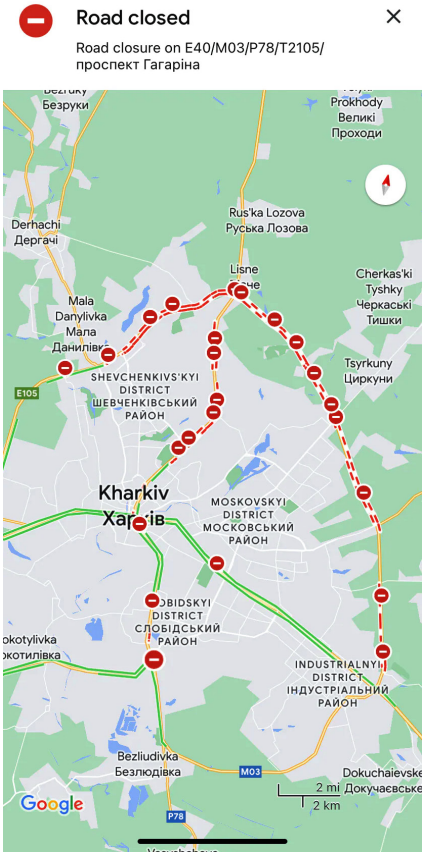
c These Japanese personnel were skilled in Bengali, Burmese, Chinese, Indonesian, Japanese, Khmer, Korean, Hindi, Malay, Nepali, Vietnamese, and a number of European languages.

# U.S. Intel: A Brief History

A big shift in US attitudes took place after the 9/11 terrorist attacks. The Intelligence Reform and Terrorism Prevention Act of 2004 called on the new Director of National Intelligence to create a "center for the collection of analysis, production and dissemination of open source intelligence to the intelligence community (IC)." It also called on the DNI to make sure that the IC made efficient and effective use of open-source information and analysis and integrate open sources into the national intelligence cycle.[12] Even before the Act came into force the Open Source Center was created in 2003 with an attached Open Source Academy to provide training to the IC.

Amy Zegart notes that "Russia's invasion of Ukraine has been a watershed moment for the world of intelligence."[13] What has been striking, however, is that the Ukraine war has led to an explosion of open-source intelligence. For example, Ukrainian forces, using social media posts, smartphone photos, commercial drone videos, commercial satellite imagery and geolocation techniques, found precise locations of Russian military forces. This is a new development in warfare that merits scrutiny. In a sense it is the first 'digital war', an interesting aspect of which is that a lot of the capability is coming from commercial services rather than the military.[14]

## Figure 1. Open-Source Maps




*Google Maps shows road closures near Kharkiv, Ukraine, at the onset of the Russian invasion in February 2021.*

*Source: Rachel Lerman/The Washington Post*[15]

At the war's onset, there was an explosion of open-source intelligence through social media posts, smartphone photos, commercial drone videos and cheap satellite imagery that provided locations of Russian military and virtually predicted an invasion.[16] The American multinational Dow Inc's resident intelligence unit tracked signs of Russia's invasion plans and in a letter to their superiors predicted the date of invasion as 23 February—all through the use of publicly available sources. This is part of a trend of companies and non-profits maintaining such capability to gain strategic and economic advantage. In Dow Inc's case it was to recommend possible escape routes for company personnel.[17]

Ukrainian forces and civilians used these networks to report on Russian movements. The Ukrainian government has taken advantage of this and have modified their sophisticated public service *Diia* app to report on the movements of enemy troops and hardware and provide 24/7 access to TV and radio. What citizens do is to provide geotagged pictures and videos which have military value.[18]

Indeed, Zegart has noted, private citizens and groups have been tracking Russian activities and journalists have used open-source imagery for reporting on the conflict. For instance, a volunteer group led by a former US Army open-source imagery analyst has provided the United Nations useful information about Russian excesses in the war, uncovering and verifying information using commercial satellite thermal and electro-optical imaging, TikTok videos, and geolocation tools.[19]

The Russian invasion has helped the emergence of what *Washington Post's* technology reporter Pranshu Verma calls "hobbyist spies," [20] or amateurs enhancing their expertise on-the-job. Some are tracking military aircraft near the border, others are using the NASA database on fires, along with contemporary satellite imagery that identifies "thermal anomalies" triggered by shelling. Verma has described the case of Kyle Glen, an amateur in the UK who, intrigued by a video he found on Telegram of the Russian Army bombing a civilian escape route, set out to verify the report. In the video footage he found a landmark—a Russian Orthodox Church with four golden domes, using Google Maps and a file photo from news wire agency AP to generate precise coordinates. Scanning Discord, Reddit

and Twitter, he obtained chatter from those who had seen the bombing at a place near Irpin. He was thus able to post the video on Twitter.[21]

In December 2022, *Washington Post* columnist David Ignatius wrote of how Ukrainian forces have been assisted by software developed by Palantir, an American OSINT company, which provides detailed digital maps overlaid with targeting intelligence gathered by overhead commercial satellites.[22] OSINT efforts, both Ukrainian and freelance, have partly been assisted by the ability to scour Telegram channels such as Rybar founded by former Russian defence ministry officials. With 1 million members, the channel has provided accurate accounts of developments in the battlefield. Telegram is itself a favourite platform of Russian ultra nationalists who are often angry at their country's performance in the war. Another similar source is VKontakte, the Russian equivalent of Facebook. Russian military personnel with no compunction about uploading photos and videos of their whereabouts have been known to compromise their forces' interest.[23]

At the same time, others are issuing warnings about what could be described as overreliance on OSINT in these circumstances. In an address before the Royal United Services Institution in London, Sir Jim Hockenhull, commander of the UK strategic command and former head of Defence Intelligence, warned against "confirmation and availability bias" in processing information gathered through OSINT.[24] He did, however, acknowledge its importance especially in countering Russian information operations and their narratives around the war. He said, "Open source contributes somewhere in the region of 20 percent of our current processes, but the availability and opportunity means we have to invert this metric." Rather than having OSINT as a mix in the base of an intelligence cake, he noted, "secrets should be the icing on an open source cake." He pointed to the need for effectively merging OSINT and traditional intelligence.[25]

# Typology of Open and Classified Information

The aim of intelligence is to obtain insight into an adversary's plans and intentions. This is often best done through clandestine means. What OSINT does is to provide a link with open sources which can supplement secret information in ways that make it more useful; it does so with greater speed. Indian intelligence officers say they prefer to use sources of provenance and that sometimes it is not clear as to the true origin of OSINT information.[26] The traditional intelligence community is careful about information it gathers as 'intelligence', ensuring that it is evaluated and verified.

Secret sources begin with the old fashioned, but still most reliable—human intelligence (HUMINT) derived through clandestine means from parties who may have been persuaded to provide it on account of blackmail, greed for money, or to settle a grievance against their superiors, or simply that it hewed to their own ideology to do so. Another type is technical intelligence (TECHINT) which focuses on obtaining information on the weapons and equipment used by adversary nations. This includes not just technology but also science, and is aimed at ensuring that a state's own forces do not have to confront any technological surprise on the battlefield. The second stage of the processing of the information obtained through testing and analysis can reveal the techniques and materials that have gone into a weapons system. In many ways, TECHINT as a discipline matured during the Second World War. The British scientist R.V. Jones' autobiography describes the role played by TECHINT in defending Britain in the grim days of 1940-41, and in the subsequent years as the war unfolded.[27]

TECHINT in the Second World War was often obtained by partisan groups and spies, but it can come in a variety of ways such as the capture of equipment on the battlefield, clandestine acquisition, or simply by accident. One of the most notable feats in Cold War history was the defection of a Soviet pilot along with his state-of-the-art MIG 25 to the West in 1976.[28]

Other ways of gathering intelligence include signals intelligence (SIGINT) which seeks to intercept communications and which began with the interception of adversary tactical wireless and shortwave radio communication. Today it includes communications intelligence (COMINT)

gathered by intercepting microwave signals or tapping undersea cables. A useful example of this was India's interception of a telephone conversation between General Pervez Musharraf, then Pakistan Army Chief who was in Beijing and its Chief of General Staff Mohammed Aziz, in Rawalpindi, which established Pakistan's complicity in the Kargil intrusion of 1999.[29]

There is also electronic intelligence (ELINT), used to gather electromagnetic signatures of radars and other sensors and build an order of battle of opposing forces. In today's world, COMINT could also involve the interception of messages through apps like WhatsApp or Telegram and Signal. Cryptanalysis is an integral part of the process since sensitive communications are often sent in code. Imagery Intelligence (IMINT), meanwhile, is aimed at analysing satellite imagery. While today, commercial companies sell ground imagery, the spy satellites of countries like the US or Russia provide images of such resolution that they can aid in providing TECHINT on the quality of enemy equipment, bridges, and airfields.

OSINT can supplement TECHINT by its ability to track scientific and technological developments quick time, with key links provided by analysts and observers who may not be professional intelligence officers but researchers and scholars who may be accessing open databases for some project of their own. Likewise, it can assist IMINT by amateurs and hobbyists scouring satellite imagery in unlikely places to come up with information of some intelligence value.

The aim of OSINT is not to replace clandestinely collected information, but to complement and supplement it. It can be an analyst's source of first resort, which helps them focus on what is classified. Thus, while basic work can be done using commercially available imagery, the intelligence agencies can use their scarce satellite resources on the higher-value targets. While the traditional forms of intelligence are important, there are some areas in which OSINT is more effective. In the last two decades, for example, news agencies like CNN or Al Jazeera have reported on military developments and terror attacks before they have been officially reported by the concerned state. There is also information that can be gleaned from Jihadi forums, which have evolved into sophisticated outlets for extremists, and have yielded information on extremist propaganda and recruitment.[30]

# Open-Source Information Vs. Open-Source Intelligence

## Information explosion

The sheer volume of information available through a multitude of open sources makes it important to separate classified from open information.

A contemporary list of what could be OSINT sources would read like the following:

1. Conventional media—i.e., newspapers, magazines, TV, and radio

2. Government data including annual reports, budgets, hearings and legislative debates, government reports such as censuses, press conferences, marine and aeronautical notifications, and public notifications of government contracts

3. Information from professional and academic proceedings like conferences and seminars, speeches, and academic and trade publications

4. Databases—geospatial data, commercial satellite imagery, scientific-technical data and commercial and economic data. These can be both commercial and public or managed by institutions like think tanks and libraries.

5. Internet—emails, blogs, social media sites like Facebook, Twitter, YouTube, TikTok, online publications and websites

6. Output of amateur groups involved in aircraft spotting, ham radios, hobbyists tracking space launches and satellites. NGOs involved in environment protection and think tanks specialising in security, energy and environment.

7. A great deal of intelligence can also be gleaned from commonly available data on weather, white shipping, Jeppsen charts in civil aviation, navigation, geodetic, human terrain and environmental data.

8. Considerable information can be obtained from the entire world of computers and cyber activities, ranging from issues relating to email breaches, phishing, to issues like the Dark Web, malicious file analysis, and exploits and advisories.

Open-source information only becomes intelligence once it is *collected, analysed and disseminated* in a timely manner. The aim of an OSINT outfit is to acquire, process and distribute open-source information. In this way, it can enable the intelligence agencies to focus on more effective and efficient use of their own unique classified assets. The guiding principle is, "We should not send a spy where a schoolboy can go."[31]

OSINT requires extensive processing and analysis. Thus there may be a need for 24x7 tracking of jihadi websites, translated transcripts of terrorist leaders' statements and speeches, and translations of their communiqués. Software is also required, like that of Visible Technologies[32] which can track posts and conversations in sites like Amazon, Flickr, and Facebook, or else software that can search for video clips of interest.

## The connectivity revolution

The connectivity revolution wrought by the Internet, which has linked computers and other electronic devices all over the world through cables and wireless, has changed the world as we know it. It has dramatically altered politics, fueled protest movements, aided repressive crackdowns, and transformed information warfare. It has changed people's daily lives in other ways in conjunction with specially devised algorithms that decide what we buy, what we read, which places we visit and, fundamentally, what we know.

Technology has dramatically altered the landscape which we need to make sense of. There are some 9 billion searches on Google every single day.[33] There is no count of how many cell phone users are recording and posting on events in real time. There are some 6,000 tweets on X (ex-Twitter) every second, or 500 million tweets a day.[34] There are some 347.3 billion emails sent per day (85 percent of which are spam), which means 4 million per

second.[35] There are some 3 billion monthly active users of Facebook;[d,36] some 350 million photos are uploaded on the platform every single day, or 4,000 photos per second.[37]

### *GEOINT*

There is another revolution that is taking place—that of geospatial information. There was a time when satellites were owned by governments, and their products, especially imagery and electronic intelligence, comprised key elements of the work of intelligence communities. Today, however, commercial firms launch scores of small satellites whose images are available in the market. Some images are now of nearly military-grade resolution.[e] Besides, they are also running constellations that are able to provide quick revisits to areas of interest.[38]

There has been a transformation of what once was the highly classified world of satellites and intelligence. Satellites have played a key role in gathering geospatial intelligence (GEOINT) since the 1960s. Photo and radar imagery were important for military purposes as well as providing data related to weather and agriculture.[39] Satellites were also used for communications and thereby emerged as a crucial source of COMINT. They were also widely used for arms control, keeping track of potential violations such as proliferation of adversary missiles or nuclear facilities.

With such capabilities, satellites were a government monopoly until the 2000s. Over time, a large number of commercial applications appeared for weather and agriculture forecasting, shipping, communications, news gathering, environment monitoring, and urban planning. This inevitably led to OSINT applications. By 2019, 25 commercial satellites were offering sub two-metre resolution– 19 of them offering less than a metre resolution, with some offering 31 cm. Government satellites, of course, have 5-10 cm resolutions which can help analysts with more difficult tasks like determining the technical parameters of a bridge or a warship. With such resolutions came an army of amateur analysts who now constitute a world of their own in OSINT.

---

d India leads the world in the number of Facebook users at 349 million.

e There are different types of resolution—radiometric, spatial, spectral and temporal. In an optical satellite what it means is that, for example, if the imagery has 1 metre resolution, each of the pixels of the image represent a 1x1 m square on the ground.

# Open-Source Information Vs. Open-Source Intelligence

Companies like the American Planet Labs now have anywhere up to 200 observation satellites circling the globe and producing a million images a day covering the entire Earth. They sell their output to their own government, but also to foreign governments close to the US, and private commercial companies and environmental organisations studying phenomena such as ice melt, aid groups that track refugee movements, and for crop monitoring.[40]

There are other improvements in satellite capabilities as well such as hyperspectral sensors that can make fine distinctions in analysing light beyond the visual spectrum, video capabilities that can track vehicle movement, synthetic aperture radars (SAR) that can penetrate clouds as well as detect micro-changes relating to tunneling and underground construction. Some satellite companies also offer high-revisit rates which help keep track of a particular development—be it construction, encampment of soldiers and equipment, or ship movements in a harbour.

Most of the leading satellite companies are offering not only imagery, but also the use of artificial intelligence (AI) and Machine Learning (ML) algorithms to automate analysis for urban planning, disaster management, and environmental impact. Besides image processing and multi-spectral analysis, they are also into creating Digital Elevation Models and 3-D Terrain Models using mono and stereo satellite imaging data. Such models use computer graphics to depict elevation or the terrain itself. From the point of view of defence and security, in essence, the GEOINT revolution ensures that you are being observed by someone or the other all the time and you have to learn how to operate in the open. This makes strategic surprise a difficult task.

# Processing OSINT

As discussed earlier in this paper, the digital universe is growing at a phenomenal speed as data accumulates from multiple sources. The point of intelligence is to make sense of this data and separate the proverbial wheat from the chaff. This is where AI comes in. AI associated with cloud computing, advanced sensors, and Big Data analytics play a role: ML algorithms can make sense of the vast amount of "news" or satellite imagery gathered; algorithms are first trained on a data set to look for specific patterns and thereafter they can track those images at computer speed.

However, using AI for data analysis is still in its infancy. As in other areas, what would still be more effective is the work done by collaboration between human and machine. As it is, in the field, there are things best done by humans such as trying to figure out adversarial intentions, and contextualising data. As noted earlier, the key to open-source intelligence is extensive processing and analysis of the data generated. With the internet providing ever greater volumes of data, it requires specialised data analytics and crawlers[f] to make sense of it. There may be specialised crawlers for specific applications and this could involve specialised processing servers that can be programmed to crawl with topic-spotting algorithms. Using ML and natural language processing (NLP), they identify patterns and trends that may not be easily visible otherwise.

Perhaps the oldest way of processing data was through the conduct of content analysis—for instance, counting the number of times an article mentions Xi Jinping as the "people's leader" or the number of times "Xi Jinping Thought" is mentioned in a speech. Advances in deep learning that uses algorithms to analyse text have enhanced the value of this kind of research and yield "intent analysis" by providing context to the message.[41]

f 'Web crawlers' are also known as robots, bots, ants or spiders. Scores of web crawlers visit websites, scan pages to create entries for a search engine's index. Search engines like Google, Bing or Baidu use crawlers to index downloaded pages so that users can have quicker and more efficient access to them.

# Processing OSINT

OSINT processing requires specialised geolocation tools to pinpoint the source of the data to make it useful for intelligence purposes. Geolocation uses location technologies such as GPS and IP addresses to identify and track the whereabouts of connected electronic devices. The process is made easier by the fact that many photos shared in the internet are encoded with metadata about the time, location and even type of camera that took the picture, as well as where and when the user uploaded it.[g]

> "The key to open-source intelligence is extensive processing and analysis of the data generated."

g With a certain amount of effort, it is possible to remove such encoding.

# OSINT in Nuclear Non-Proliferation

One area in which OSINT has already made a mark is in non-proliferation. Well-funded think tanks and some commercial companies in the US and Europe have made effective use of the internet and data revolution. A pioneer is Jeffery Lewis, Director of the East Asia Non-Proliferation Program at The James Martin Center for Non-Proliferation Studies. In 2021, Lewis detailed the new tools that were used by him and other analysts to debunk a claim by Iranian dissidents about a secret nuclear facility in Teheran. Earlier, in 2009, they were also able to prove that what media reports had alleged to be a nuclear facility in Syria was a textile factory.[42] No doubt the US intelligence agencies would have known this, but they were not in the debate played out in the media. Though governmental agencies have also been proven to be spectacularly wrong, as was the case in the so-called Iraqi nuclear weapons that were used to launch the second Gulf War against Iraq.[43]

At the same time, amateurs have made certain important discoveries. For example, in 2012, Siegfried Hacker and Frank Pabian, researchers at Stanford University's Center for International Security and Cooperation, were able to determine the location and supporting structures of North Korea's first two nuclear tests through commercial imagery and seismological information. North Korea would confirm this six years later.[44]

From the Indian point of view, there have been some interesting applications in the context of proliferation and non-proliferation. In 2009, Hans Kristensen, analyst at the Federation of American Scientists (FAS), posted what appeared to be a fairly definitive picture of a Pakistani nuclear storage site near the Masroor Air Base 12 km from Karachi.[45] Later he made a more extensive analysis of Pakistan's evolving nuclear weapons infrastructure.[46]

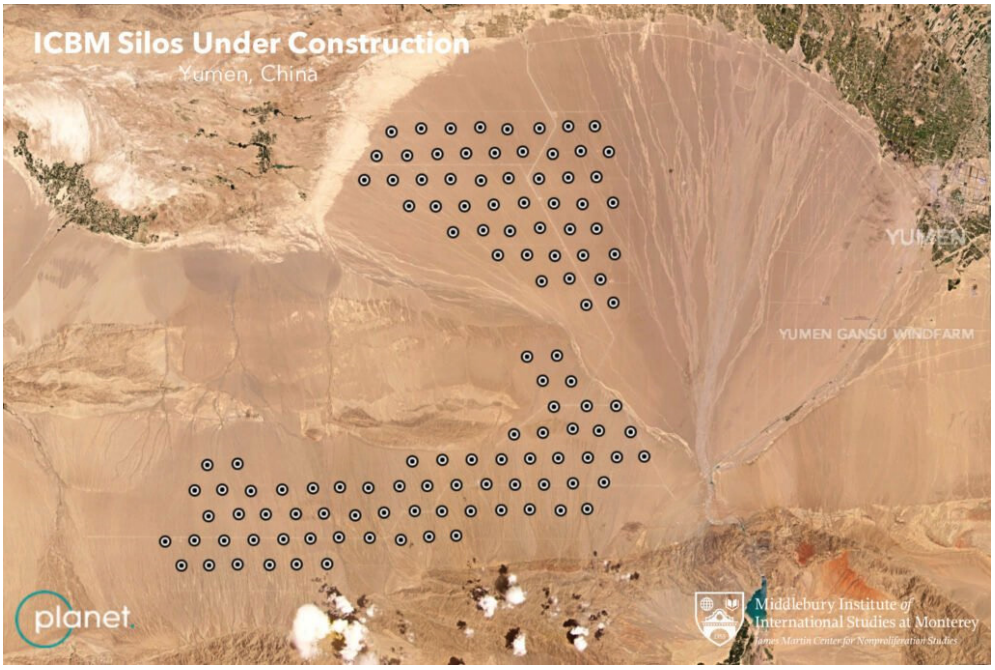
## Figure 2. Satellite Images


*Source: Federation of American Scientists*

In 2015, the Institute for Science and International Security posted an analysis arguing that Pakistan's Chashma plutonium separation plant had possibly become operational.[47] This had important implications for Islamabad's ability to boost its nuclear weapons holdings. Some years later, in 2021, a more dramatic series of revelations ensued when satellite images taken by Planet Labs and analysed by Decker Eveleth[h] indicated that China was significantly expanding the number of silos for intercontinental range ballistic missiles (ICBMs) at Yumen in Gansu province.[48] This would have doubled the official estimate of Chinese ICBMs.

h At that time, he was interning at the James Martin Center for Nonproliferation Studies at the Middlebury Institute for International Studies, Monterey. He is currently Graduate Research Assistant there.

## Figure 3. Planet Labs Satellite Images




*Source: Middlebury Institute for International Studies, Monterey, Calif. USA.*

Yet, there was more to come. Soon after, on 26 July, Matt Korda, a researcher at the FAS announced their discovery of an additional 110 missile silos at Hami on which construction had begun in March 2021. There is a potential third site at Hanggin Banner, Inner Mongolia, which was disclosed in a report of 12 August.[49]

To be sure, government agencies have a more accurate picture than those drawn by non-government analysts. They do not just give it away freely, however. Owing to the data made available by the non-government analysts, the notion that China is expanding its ballistic missile arsenal has entered the public policy discourse, which would have otherwise had to wait for an official government statement.

# The Amateur's Edge

Hobbyists and enthusiasts play an important role in gathering and processing OSINT, as described earlier in the paper in the context of the conflict in Ukraine. According to certain media accounts, tracking by hobbyists began with the Arab Spring in 2011 when smartphones and social media entered the fray.[50] They also tracked the 2014 Russian invasion of Crimea and the 6 January 2021 riot in the US Capitol.

There are many communities who use chat rooms, Twitter and YouTube channels to interact with each other to share knowledge and solutions. One such, called The OSINT Curio.us Project (TOCP), was launched in 2018 from the Dutch town of Papendal but has now shut down. Their self-assigned goal was to teach people the basics of OSINT and investigating techniques.[51] The internet also has a range of OSINT tools to help analysts. There is an OSINT Framework that helps OSINT analysts organise and manage their research. The framework is free and can be customised to meet individual needs. Babel X, a cloud-based service, uses AI to cross language barriers for any search term. Google Dorks is an OSINT gathering method using special search queries of the Google database to obtain information. Maltego is an OSINT tool for gathering information and bringing it together in a graphical correlation analysis. Aircrack-ng is a wifi network security testing and cracking tool that can be used both defensively and offensively to find compromised networks.[52]

Some effort has been put in by government and public institutions in the US. For example, the OSINT Academy is a collaboration between the Dakota State University and the National Security Agency and the Hetherington Group whose aim is to provide widespread cyber intelligence instruction.[53] It runs an online course that teaches the basics of OSINT. In this context, a blog that has also come into prominence in the context of the Ukraine war is Oryx or Oryxspionkop, a Dutch OSINT company which began as a group of hobbyists and whose meticulous detail of material losses in the war is based on carefully geolocated visual evidence—gathered through satellites or social media.[i,54]

i As of writing, the blog, which was run as a personal enterprise may shut down in October 2023.

Another institution in this context are Discord Servers which are organised into topic-based channels where one can interact and collaborate with the like-minded. There are at present seven different groups on Discord.[55] A similar function is played by Slack, which facilitates communication through voice and video calls, files, and text messaging, and also enables private chats or through communities called "workspaces"; it has chat rooms or channels organised by topic, and hosts private groups as well.[56]

## Commercial OSINT

The Internet era has also led to thousands of companies devising software and providing platforms for the acquisition and analysis of data. They are equipped to uncover relationships between all types of data objects such as suspects, organisations, addresses, phones, ID numbers, vehicles and finances. These have algorithms to visually show networks of related data, weighted groups of relationships, value occurrence, frequency, patterns of activity, and event sequences. Further, they can plot geographic data on a variety of built-in and user-defined graphical maps. They have the ability to monitor data sources and alert users of data changes based on user-defined criteria.

A great deal of this has been developed for commercial purposes by Big Tech like Google and Facebook. Geolocation, for example, is used to help prevent fraud, track cargo shipments, or consumer preferences. Google will collect data through web-tracking technologies such as IP address tracking, cookies and others used in the ad tracking industry. Google offers the Google Analytics platform for gleaning insights that may be useful for your business.

Among their competitors are companies like Maxar,[57] BlackSky,[58] Satellite Imaging Corporation,[59] the Chinese company Zhuhai Orbita Aerospace Science and Technology,[60] and SCS Space in South Africa,[61,62] who provide design and manufacturing for satellite and spacecraft components, as well as earth observation and exploration data using their own constellation of satellites. In many cases they also process the data and offer products to consumers who could be urban planners, environment activists,

newspapers, researchers and even governments who want to supplement data obtained through their own classified satellites.

Planet Labs, for example, mentioned earlier in this paper is one of the world's biggest providers of commercial imagery. Its website boasts having "revolutionized the Earth observation industry, [is] democratizing access to satellite data beyond the traditional agriculture and defense areas."[63] Companies like Satellogic[64] are also offering "autonomy"—i.e., one can own and task a satellite which can be deployed within three months.

Maxar is perhaps the largest of these companies which is into the design and manufacture of satellites and components for communications, earth observation and exploration. It claims to have the world's most advanced constellation covering 60 percent of the Earth monthly through high-resolution satellites. It also claims to have the largest imagery archive.[65] Most of the imagery related to the Galwan incident in 2020 was provided commercially by Maxar.

Another such company that claims to provide real-time geospatial intelligence is BlackSky of Herndon, VA. BlackSky imagery was used by *Naval Technology* magazine to cover Operation Kaveri, the Indian Navy's evacuation of refugees from Port Sudan in April 2023.[66] BlackSky has a constellation of 14 fast-response satellites orbiting along the equator and can handle imagery requests in as little as 90 minutes.[67]

Capella Space, meanwhile, is an American space company which has developed space-based radar earth observation satellites with a synthetic aperture radar (SAR) that can penetrate clouds and also work at night.[68] Capella also provides on-demand and self-service approach by providing its customers direct access to Capella's constellation tasking—in other words, an anonymised and secure tasking that is fully automated.[69] A similar company is ICEYE, a Finnish micro-satellite maker spun off from Aalto University that also specialises in SAR imagery and tracks natural catastrophes across the world. It also provides ownership of satellites that can be launch-ready between 15-24 months.[70]

Besides the companies which are providing imaging and spacecraft services, there are those like Orbital Insight, based in Palo Alto, who are into analysing the geospatial data. Their Orbital Insight GO is an AI-powered Geospatial Analytics platform designed to simplify the use of location data by allowing users to query the location data with three parameters—"what type of activity", "where on Earth", and "when".[71] This can be used for a range of applications such as supply chain intelligence, energy and industrials, financial services, and defence intelligence.

Commercial OSINT is also available through the better-known Google Search whose Google Scholar version provides data on research publications. DataSift, now acquired by Meltwater enables organisations to identify and extract insights from all types of human generated data. Visible Technologies, Trackur, Attentio, Zignal Labs, Dezzai, Neticle Labs, and Citibeats, among others, can track posts and conversations in sites like Amazon, Flickr, and Facebook. Many of these are used by companies to keep track of the activities of their competitors but they have obvious OSINT applications.

They have a geopolitical function as well. Specialised tools developed by companies like Maltego and TheHarvester can be used for OSINT and forensics. There are a number of other tools like Nmap and Metasploit, Burp suite, Wire Shark, Aircrack-ng, John the Ripper, SQLmap, and Kali Linux which can act as open-source counter-intelligence ware and are used to detect hacking, secure vulnerabilities, and exploit breaches. A lot of their work also interfaces with sentiment analysis which identifies and extracts subjective information in source material and helps business understand social sentiment of their brand, product or service from online conversations. This has similar applications in understanding political sentiments.

## Specialised OSINT companies and institutions

Jane's Fighting Ships is perhaps one of the oldest OSINT companies that spawned the Jane's Information Services group which describes itself as "the trusted global agency for Open-Source Defence Intelligence."[72] The think tank, International Institute for Strategic Studies (IISS) in London

maintains an authoritative online database on the military capabilities and defence economics of over 170 countries and issues an annual *Military Balance* publication.[73] For its part, the Stockholm International Peace Research Institute (SIPRI) has databases on arms transfers, arms industries, multilateral peacekeeping operations, and military expenditures. It also publishes an annual *Yearbook* focusing on armaments, disarmament and security.[74]

In recent decades, the explosion of data and the development of specialised intelligence analytics has been used to bring out useful OSINT in a range of areas including defence and security. The line between commercial and geopolitical intelligence is thin and many companies have emerged to service both needs. Companies like IHS Markit—now part of S&P Global—is a provider of critical information and analytics and solutions to both financial markets and governments and has a presence across the world.[75] Companies like BlackRock provide investment, advisory and risk management services which are based on open-source financial intelligence.

There is a string of other companies dealing with what is often called 'threat intelligence' and cyber security. These include Palantir, CrowdStrike, NTS, Talos, Cybersixgill, and Recorded Future (RF), which is a leader in this field and has a large team of analysts and experts in collecting and analysing OSINT data. RF has collected, structured and analysed data from the internet to create an intelligence graph that helps it to turn large amounts of data into actionable insights and develop complete, accurate and timely intelligence.[j,76]

In 2019, when the campaign against Huawei was taking shape in the US, Patricia Moriuchi of RF authored a report outlining the "corporate and personal consumer risks" that would arise from Huawei building the world's 5G networks.[77] The study included a detailed analysis of the physical global internet and Huawei's salience in the area of undersea cables, internet devices, and traffic routing.

j RF claims to be "the world's largest intelligence company" with a client base of 1,500 in 66 countries including governments and corporations.

Palantir is the Big Data analytics company whose software is being used for targeting in Ukraine, is also used by governments, intelligence agencies and businesses to track threats and make investment decisions. Palantir boasts of powering AI-assisted decision-making "from war zones to factory floors."[78] Bellingcat is another company that has grown in recent decades. It uses open-source intelligence for investigative journalism that includes incidents like the shooting down in 2014 of Malaysia Airlines flight MH 17 with an anti-aircraft missile by pro-Russian Ukrainian separatists.[79] It is also known for having uncovered Russia's role in the attempted murder of Sergei and Yulia Skripal in the UK and Alexei Navalny in Russia.[80]

## Recent Developments in the US

By 2005 the FBIS had been merged with the Open Source Center, managed by the CIA, but a component of the Office of the DNI. They created an online news service called World News Connection (WNC) that operated through the NTIS, offering the translations and information compiled around the world from news agencies, newspapers, radio and TV stations.[81] Though its public offering was a limited feed, as compared to what was available to US government users, it was an invaluable service. But in 2013 the WNC was terminated and the Open Source Center stopped providing its information to the public.[82] In 2015, it became the Open Source Enterprise (OSE) and was absorbed into the CIA's Directorate of Digital Innovation. In 2019 the OSE decommissioned its website and made it products difficult to access.

In September 2021, the US House of Representatives directed the Secretary of Defense and the Director National Intelligence to "implement a plan to elevate open-source intelligence to a foundational intelligence for strategic intelligence that is treated on par with information collected from classified means for example, human intelligence, signals intelligence and geospatial intelligence." A subsidiary aim was to also use unclassified intelligence "to combat threats from disinformation and misinformation."[83]

Speaking to the Subcommittee on Intelligence, Information, and Terrorism Risk Sharing on 21 June 2005, its chairman Rob Simmons told his colleagues that the DHS produced an open source infrastructure report to critical infrastructure owners and operators.[84]

# The Amateur's Edge

What the data explosion has done is to compel the US official intelligence agencies to reach out to the commercial sector. In May 2022, it was announced that the US National Reconnaissance Office would provide billions of dollars to the well-known companies like BlackSky, Planet and Maxar over the next ten years. An official press release noted that this was in line with the NRO's "long standing strategy of 'buy what we can, build what we must'." Actually, these commercial GEOINT companies were now putting up far more assets into space than NRO had done in the past decades.[85]

> "The line between commercial and geopolitical intelligence is thin and many companies have emerged to service both needs."

In India, as elsewhere, unclassified information is easily dismissed by intelligence professionals, in some cases justifiably so because it is difficult to verify. Even so, this paper has outlined why the time has come to systematically collect and analyse open-source information, transform it into high-quality OSINT, and be made a component of analytical reports of intelligence agencies.

So far, a great deal of OSINT analysis relating to India is being done abroad. A notable name in this regard is Nathan Ruser of the Australian Strategic Policy Institute who has put out reports and analyses based on satellite imagery relating to the Sino-Indian clash in Galwan in 2022 and the more recent one in Yangtse near Tawang.[86] Ruser is also the analyst who showed, through OSINT methods, how the IAF bombs missed their targets in Balakot.[87]

## Figure 4. India's Balakot Miss


*Source: Satellite imagery © 2019 DigitalGlobe, a Maxar Technologies company—provided by European Space Imaging.*

There is also the work by Robert Barnett on the Chinese construction of the so-called Xiaokang villages in Bhutanese territory.[88] Equally important are OSINT analyses, one on the orbat on the Sino-Indian border by the Belfer Center,[89] and the other by Stratfor analyst Sim Tack explaining China's infrastructure build-up along the border.[90]

As of now there seems to be little available from Indian analysts and think tanks. A start has been made by the Bengaluru-based think tank, Takshashila Institution, which has a strong China-focused team with Manoj Kewalramani producing a translation of *People's Daily* every day. There is also the weekly *Eye on China* bulletin which focuses on a range of issues from defence and security to domestic politics and economics. Recently some more new products have emerged from the Takshashila which would definitely classify as OSINT and could mark the beginning of an Indian foray into this area.[91] Suyash Desai, who was one of the authors of the Eye on China bulletin, is now a scholar with the National Taiwan Normal University and brings out the PLA Bulletin in Substack.[92]

At present, India lacks the ecosystem in which hobbyists like flight trackers, plane spotters, satellite imagery enthusiasts who have graduated to the level of think tanks and have interacted with official agencies to provide rudimentary OSINT. While a few retired analysts have contributed to the media on IMINT analysis, there has been little else.[93] There is a vital learning link that needs to exist between retired government analysts and non-official analysts, but that may now have been blocked by regulations prohibiting intelligence personnel from writing freely in the media.

## Figure 5. Recent Clashes in the Yangtse Region Near Tawang

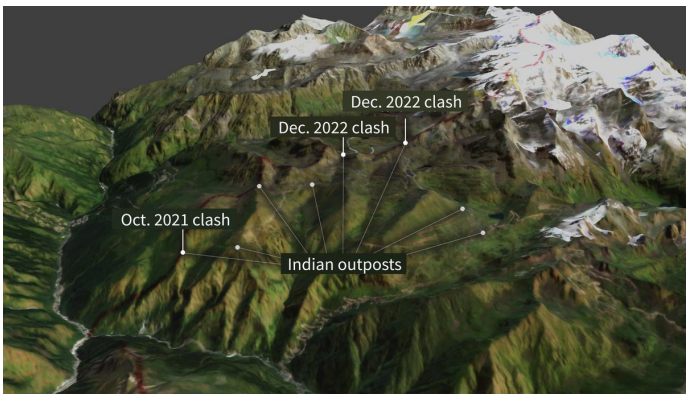



*Photo Credit: ASPI and Planet Labs*[94]

There is a large technology-savvy community of young people in India specialising in software and communications, and who may have the knowhow to birth an Indian OSINT community. This will require, however, some assistance from the government which needs to rethink certain rules and regulations that, for example, prohibits non-government people from accessing classified information. Having civilian contractors or even amateurs collaborating on OSINT issues with the government would require a new approach.

Indian intelligence agencies, like such outfits elsewhere, operate in stovepipes. Yet, as this analysis has suggested, this is a new era where data and information of importance to intelligence, in the classical sense, is all around us, all the time. We need to understand this and figure out ways of accessing and effectively utilising it.

India has a developed space industry, but it is no match for its large and vibrant American counterpart. India has its own set of satellites which are for Earth Observation and has associated establishments like the National Technical Research Office (NTRO) and the Defence Imagery Processing and Analysis Centre (DIPAC) for intelligence purposes. The National Remote Sensing Centre in Hyderabad and its associated Regional Remote Sensing Centres receive, process and disseminate imagery acquired from Indian civilian satellites. There is no reason why some way could not be found to create a community of non-governmental persons interested in OSINT using some of this imagery.

India has used commercially available imagery for intelligence purposes, such as the access to SPOT of France in the 1990s, or the Israeli-built TechSar synthetic aperture radar satellite in the mid-2000s. In the area of OSINT, as discussed earlier, satellites and constellations can be hired and the data processed as per requirements. Of course, the challenge is not just from GEOINT, but the entire spectrum of data and information available today. The challenge is not only to access data and process it, but also protect it from those seeking to misuse it.

Those involved in classified intelligence have dedicated agencies of their own, such as the Research & Analysis Wing (R&AW), Intelligence Bureau (IB), the military and the various financial intelligence outfits. Expecting them to treat OSINT on a par with their own information is an uphill climb. That is, however, what the US House Subcommittee recommended to the even better funded and capable US intelligence community.[95]

# Recommendations and Conclusion

The first challenge is to create an ecosystem of non-government students, hobbyists and enthusiasts, and interest them in the fields that can be used for OSINT. This must necessarily be a bottom-up effort. A helping hand could be provided through the National Cadet Corps or the National Social Service schemes. At a higher level, think tanks can be encouraged to create cells of analysts who can use unclassified imagery, data and social media output to make social, ecological or geopolitical reports. The government can support this process by identifying and strategically funding some of the research institutions.

A second strand could be to link the public sector, which for the present has a monopoly on Indian satellite imagery with think tanks and even private sector companies in training a new generation of analysts who can then provide the necessary impetus to the development of OSINT in India.

Another stream of effort can come from the government itself. In the short term, it may be a good idea for the National Security Council Secretariat to create an Open Source Centre and create an interface with existing agencies like R&AW, NTRO, ISRO, and DIPAC to assist the process, along with links with private sector companies dealing with information and analytics. This could be associated with an effort to form government agencies like NTRO and the NSCS to create platforms where they can associate with the non-government analysts and the hobbyists community. Connectivity is a network which is rapidly filling up the ocean of information faster than can be handled. There was a time when information was a scarce and jealously guarded commodity, but in the current era, sharing can often add greater value.

# Recommendations and Conclusion

This paper's aim was to introduce the concept of Open Source Intelligence to a largely Indian audience. The aim was to enable an understanding of the vast potential that OSINT offers for both non-governmental research, as well as for use in national security. As has been shown, this is an age where information is overflowing the banks. Official agencies dedicated to intelligence work would benefit from effectively supplementing their work with OSINT. For this the imperative is an ecosystem of amateur enthusiasts and research scholars as well as think tanks and institutions who can refine OSINT techniques and disseminate its products. This requires certain guidance and direction, as well as some funding to seed the process.

**Dr Manoj Joshi** *is Distinguished Fellow at ORF.*

# Endnotes


1 Office of Public Affairs, Central Intelligence Agency, *A Consumer's Guide to Intelligence* (Washington DC, 1999) pp. vii https://ia800601.us.archive.org/26/items/consumersguide_tenet/consumersguide_tenet.pdf

2 Heather J Williams, Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, (Santa Monica, RAND, 2018) Introduction pp. 1

3 Williams and Blum, *Defining Second Generation*

4 Amy Zegart, *Spies, Lies, and AI Gorithms: The history and future of American intelligence*, (Princeton, Princeton University Press, 2022) pp. 4

5 Office of Inspector General, Department of Homeland Security, *The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting*, July 6, 2022, https://www.oig.dhs.gov/sites/default/files/assets/2022-07/OIG-22-50-July22.pdf

6 Zoe Haver, Inskit Group, "Private Eyes: China's Embrace of Open-Source Military Intelligence" *Recorded Future,* June 1, 2023, https://www.recordedfuture.com/private-eyes-chinas-embrace-open-source-military-intelligence. Inskit Group is the threat research division of the company.

7 Lin Yang, "China to limit access to largest academic database," *VOA*, March 30, 2023, https://www.voanews.com/a/china-to-limit-access-to-largest-academic-database-/7029581.html

8 CIA, *A Consumer's Guide to Intelligence*, p.2

9 Joseph E Roop, *Foreign Broadcast Information Service: History Part I 1941-1947* (Central Intelligence Agency, April 1969), https://www.cia.gov/readingroom/sites/default/files/FBIS_history_part1_0.pdf

10 David A Reese, "50 Years of excellence: ASD forges ahead as the Army premier OSINT unit in the Pacific," *Military Intelligence*, vol 31 No 4, October-December 2005 pp 27-29, https://irp.fas.org/agency/army/mipb/2005_04.pdf

11 Detail of JPRS in Rutgers University Library online catalogue, https://www.libraries.rutgers.edu/databases/jprsx#

12 "Revised definition of national intelligence," Intelligence Reform and Terrorism Prevention Act, Public Law 108-458, December 17, 2004 Section 1012, https://www.govinfo.gov/content/pkg/PLAW-108publ458/html/PLAW-108publ458.htm

13 Amy Zegart, "Open Secrets: Ukraine and the next intelligence revolution," *Foreign Affairs*, January-February 2023 (published on 20 December 2022)

# Endnotes

14 David Barno and Nora Bensahel, " The other big lessons that the U.S. Army should learn from Ukraine," *War on the Rocks*, June 27, 2022, https://warontherocks.com/2022/06/the-other-big-lessons-that-the-u-s-army-should-learn-from-ukraine/

15 Rachel Lerman, "On Google Maps, tracking the invasion of Ukraine," *Washington Post*, February 27, 2022, https://www.washingtonpost.com/technology/2022/02/25/google-maps-ukraine-invasion/

16 "Open-source intelligence is piercing the fog of war in Ukraine," *The Economist*, January 13, 2023, https://www.economist.com/interactive/international/2023/01/13/open-source-intelligence-is-piercing-the-fog-of-war-in-ukraine

17 Warren P Strobel, "Rise of Open-Source Intelligence tests U.S. spies," *The Wall Street Journal*, December 11, 2022, https://www.wsj.com/articles/rise-of-open-source-intelligence-tests-u-s-spies-11670710806

18 Craig Turp-Balazs, "In Ukraine, the process of digitalization continues, even under cruise missile attack," *Emerging Europe,* March 29, 2022, https://emerging-europe.com/news/ukraine-vows-to-make-russia-pay-for-economic-cost-of-its-invasion-while-diia-app-proves-its-worth/

19 Zegart, "Open Secrets: Ukraine and the next"

20 Pranshu Verma, "The rise of the Twitter spies," *Washington Post*, March 23, 2022, https://www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence-ukraine/

21 Verma, "The rise of the Twitter spies"

22 David Ignatius, "How the algorithm tipped the balance in Ukraine," *Washington Pos*t, December 19, 2022, https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

23 "Open-source intelligence is piercing the fog of war…."

24 "How Open-Source intelligence has shaped the Russia-Ukraine war," An address by Sir Jim Hockenhull at the Royal United Services Institution, November 7, 2022, https://www.rusi.org/events/members-events/how-open-source-intelligence-has-shaped-russia-ukraine-war

25 "How Open-Source intelligence has shaped the Russia-Ukraine war"

26 Personal conversation with two former intelligence officers

27 See R.V. Jones, *Most Secret War: British Scientific Intelligence 1939-1945* (London, Hodder & Stoughton, 1985)

# Endnotes

28 Stephan Wilkinson, "The MIG-25 terrified the West until a defector exposed its true nature," *History.net,* July 20, 2022, https://www.historynet.com/mig-25/

29 Excerpts of conversation between Gen Musharraf and Lt Gen Aziz, *Rediff on the Net,* June 11, 1999, https://m.rediff.com/news/1999/jun/11talk.htm

30 See "Jihadist use of Social Media—How to prevent terrorism and preserve innovation," *Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security, House of Representatives, One hundred and twelfth Congress First Session December 6, 2011* (Washington DC, Government Printing Office, 2011)

31 Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, VA, USA, AFCEA International Press, 2000) p. 69

32 See profile of Visible Technology in CBInsights https://www.cbinsights.com/company/visible-technologies

33 Jason Wise, "How many Google Searches per day in 2023? (Full statistics)", *Earthweb*, May 10, 2023, https://earthweb.com/how-many-google-searches-per-day/

34 Jack Shepherd, "23 essential Twitter statistics you need to know in 2023," *Social Shepherd*, May 16, 2023, https://thesocialshepherd.com/blog/twitter-statistics

35 Wise, "How many Google Searches "

36 Shepherd, "23 essential Twitter statistics"

37 "41 Up-to-date Facebook facts and stats," *Wishpond Blog*, https://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats#:~:text

38 Zegart, *Spies, Lies, and Al Gorithms*, pp. 6

39 "What do we use satellites for?" Educational Graphic by Rocket Lab, https://www.rocketlabusa.com/assets/Uploads/RL-EducationGraphics-Satellites-today.pdf

40 Greg Myre, "A Spy Agency's Challenge: How to sort a million photos a day, " *NPR,* March 12, 2020, https://www.npr.org/2020/03/12/807499102/a-spy-agencys-challenge-how-to-sort-a-million-photos-a-day

41 See Columbia University, Mailman School of Public Health, " Content Analysis," https://www.publichealth.columbia.edu/research/population-health-methods/content-analysis#:~:text .

42 Jeffery Lewis, "Applying New Tools to Nonproliferation: A nuclear detective story," Nuclear Threat Initiative Resource Collection, September 20, 2021, https://www.nti.org/analysis/resource-collections/applying-new-tools-to-nonproliferation-a-nuclear-detective-story/

# Endnotes

43 Nomaan Merchant, "Iraqi WMD failures shadow US intelligence 20 years later," *AP News*, March 23, 2023, https://apnews.com/article/iraq-war-wmds-us-intelligence-f9e21ac59d3a0470d9bfcc83544d706e

44 Cited in Zegart, *Spies, Lies and Al Gorithms* pp. 241.

45 Hans Kristensen, "Pakistani Nuclear Forces 2009" *Federation of American Scientists*, August 28, 2009, https://fas.org/publication/pakistan2009/

46 Hans Kristensen, "Pakistan's evolving nuclear weapons infrastructure," *Federation of American Scientists*, November 16, 2016, https://fas.org/publication/pakistan-nuclear-infrastructure/

47 David Albright and Serena Kelleher-Vergantini, "Pakistan's Chashma Plutonium Separation Plant: Possibly operational," *Institute for Science and International Security*, February 20, 2015, https://isis-online.org/isis-reports/detail/pakistans-chashma-plutonium-separation-plant-possibly-operational/12

48 Jeffrey Lewis, "Chinese ICBM Silos," July 2, 2021, https://www.armscontrolwonk.com/archive/1212340/chinese-icbm-silos/ ; See also "Open-source intelligence challenges state monopolies on information," *The Economist*, August 7, 2021, https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information

49 Shannon Bugos and Julia Masterson, "New Chinese Missile Silo Fields Discovered," *Arms Control Association*, September 2021, https://www.armscontrol.org/act/2021-09/news/new-chinese-missile-silo-fields-discovered

50 Verma, "The rise of Twitter spies…"

51 "We will always be OSINTCurio.us" https://www.osintcurio.us/2023/02/27/our-last-post/index.htm , see also https://twitter.com/osintcurious?lang=en

52 Liku Zelleke, "The best OSINT Tools,"*Comparitech*, July 13, 2023, https://www.comparitech.com/net-admin/osint-tools/

53 https://osintacademy.com/

54 https://www.oryxspioenkop.com/

55 https://discord.com/servers?

56 https://slack.com/intl/en-in

57 See Maxar, "Assured and Agile Geoint" https://betterworld.maxar.com/ ; Maxar's principal satellite is the Worldview with a 31cm resolution. It is the only commercial satellite with this capability.

# Endnotes

58 https://www.blacksky.com/company/#

59 https://www.satimagingcorp.com/about/

60 https://www.obtdata.com/en/about.html

61 https://www.scs-space.com/

62 Planet Lab Competitors and similar companies, *Craft* https://craft.co/planet-labs/competitors

63 https://www.planet.com/company/ The company uses its 200 Dove satellite constellation to generate 3-5m resolution images. Planet has archived more than 1 billion images, all them optimized for machine learning. AI plays a major role in value adding to its 600,000 images it captures daily. Patrick Moorhead, "Planet is the most differentiated space play we have researched in years, delivering daily whole earth data subscriptions," *Forbes,* November 18, 2021, https://www.forbes.com/sites/patrickmoorhead/2021/11/18/planet-is-the-most-differentiated-space-play-we-have-researched-in-years-delivering-daily-whole-earth-data-subscriptions/?sh=2f1be2ea1278

64 https://satellogic.com/company/about-us/

65 https://www.maxar.com/constellation

66 Andrew Salermo-Garthwaite, "Kaveri: Exclusive satellite imagery of India's evacuation of sudan," *Naval Technology*, April 26, 2023, https://www.naval-technology.com/news/kaveri-exclusive-satellite-imagery-of-indias-evacuation-of-sudan/?

67 See https://www.blacksky.com/

68 https://www.capellaspace.com/about-us/

69 https://www.capellaspace.com/data/constellation-tasking/

70 https://www.iceye.com/

71 https://orbitalinsight.com/

72 https://www.janes.com/

73 https://www.iiss.org/en/the-military-balance-plus/

74 https://www.sipri.org/databases

75 "IHS Markit Ltd company profile," GlobalData, https://www.globaldata.com/company-profile/ihs-markit-ltd/

76 https://www.recordedfuture.com/company

# Endnotes

77 Priscilla Moriuchi, "The New Cyber Insecurity: Geopolitical and supply chain risks from Huawei monoculture," Recorded Future Blog, June 10, 2019 https://www.recordedfuture.com/huawei-technology-risks/ Moriuchi was the Director of Strategic Threat Development at Recorded Future. Currently she works at Threat Intelligence with Apple.

78 https://www.palantir.com/

79 Bellingcat Investigation Team, "Origin of the Separatists' Buk: A Bellingcat investigation", *Bellingcat*, November 8, 2014, https://www.bellingcat.com/news/uk-and-europe/2014/11/08/origin-of-the-separatists-buk-a-bellingcat-investigation/

80 Eliot Higgins, "How Bellingcat uncovered Russia's secret network of assassins," *Wired*, February 2, 2021, https://www.wired.co.uk/article/russia-bellingcat-poison

81 University of Delaware, "World News Connection," https://library.udel.edu/databases/wnc/#:~:text=World%20News%20Connection%20is%20an,and%20radio%20and%20television%20stations

82 Stephen Aftergood, "CIA halts public access to Open Source Service," Federation of American Scientists blog, October 8, 2013, https://fas.org/blogs/secrecy/2013/10/wnc-ends/

83 US House of Representatives, National Defense Authorization Act for Fiscal Year 2022 (HR 4350). Section 1612 "Strategy and Plan to Develop Certain Defense Intelligence Reforms," *Congressional Record*, Volume 167, Number 163, September 21, 2021, https://irp.fas.org/news/2021/09/intel-reforms.html

84 US House of Representatives, "Using Open Source Information Effectively", *Hearing before the Subcommittee on Intelligence Information Sharing and Terrorism Risk Assessment of the Committee on Homeland Security,* June 21, 2005, https://www.govinfo.gov/content/pkg/CHRG-109hhrg24962/html/CHRG-109hhrg24962.htm#:~:text=Open%2Dsource%20intelligence%2C%20or%20OSINT,critical%20infrastructure%20owners%20and%20operators

85 David Coldewey, "Spy agency pumps billions into orbital imagery companies BlackSky, Maxar and Planet," *Tech Crunch,* May 25, 2022, https://techcrunch.com/2022/05/25/spy-agency-pumps-billions-into-orbital-imagery-companies-blacksky-maxar-and-planet/

86 Nathan Ruser and Baani Grewal, "Explained: The escalation on the India-China border," *The Hindu*, January 8, 2023, https://www.thehindu.com/news/national/explained-the-escalation-on-the-india-china-border/article66350993.ece

87 Marcus Hellyer, Nathan Ruser and Aakriti Bachhawat, "India's strike on Balakot: a very precise miss ?" Australian Strategic Policy Institute: *The Strategist*, March 27, 2019, https://www.aspistrategist.org.au/indias-strike-on-balakot-a-very-precise-miss/

# Endnotes

88 Robert Barnett, China is building entire villages in another country's territory," *Foreign Policy*, May 7, 2021, https://foreignpolicy.com/2021/05/07/china-bhutan-border-villages-security-forces/

89 Frank O'Donnell and Alex Bollfrass, "The Strategic Postures of China and India: a visual guide", Report of the Belfer Centre for Science and International Affairs, Harvard University, March 2020, https://www.belfercenter.org/sites/default/files/2020-03/india-china-postures/China%20India%20Postures.pdf

90 Sim Tack, "A Military Drive spells out China's intent along the Indian border", *Real Clear World* , September 22, 2020, https://www.realclearworld.com/articles/2020/09/22/a_military_drive_spells_out_chinas_intent_along_the_indian_border_578286.html? Originally published in *Stratfor Worldview*

91 See: https://trackingpeoplesdaily.substack.com/; https://eyeonchina.substack.com/

92 Anushka Saxena, "China's approach to military unmanned aerial vehicles and drone autonomy," Takshashila Discussion SlideDoc, Takshsashila Institution, September 28, 2023; https://takshashila.org.in/research/takshashila-slidedoc-chinas-approach-to-military-unmanned-aerial-vehicles-and-drone-autonomy; Dr Nithiyanandam, "#4Rapid military infrastructure expansion in Tibet: A strategic analysis," Takshashila Geospatial Bulletin, September 30, 2023, https://substack.com/inbox/post/137539829

93 See for example the work of Col (retd) Vinayak Bhatt "Infrastructure in Tibet gets a big boost as China stepped up focus after Doklam face-off," *The Print*, November 29, 2019, https://theprint.in/defence/infrastructure-in-tibet-gets-a-big-boost-as-china-stepped-up-focus-after-doklam-face-off/327698/

94 Nathan Ruser and Baani Grewal, "The latest flashpoint on the India-China border: Zooming into the Tawang border skirmishes," Australia Strategic Policy Institute, December 20, 2022, https://www.aspi.org.au/report/latest-flashpoint-india-china-border-zooming-tawang-border-skirmishes

95 US House of Representatives, "Strategy and Plan to develop certain Defense Intelligence reforms…"

*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