CENTRE FOR SECURITY STUDIES | ISSUE BRIEF

November 2022

DEVELOPING THE ROLE AND IMPACT OF OSINT ON SECURITY PLANNING

Kanak Mohiley

Edited by: Ishani Sharma

About the Author

Kanak Mohiley is a student at the Jindal School of International Affairs and is a Research Intern at the Centre for Security Studies, JSIA.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof Dr Pankaj K Jha. Researchers at CSS – through in-depth analysis briefs and events, reports, policy briefs and print publications – explore both regional and thematic topics in the broader field of international security studies. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian and religious conflict; civil wars and state failure; cyber and space warfare; resource related security issues; the proliferation of weapons of mass destruction; defence economics and also the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:

www.linkedin.com/company/jindal-centre-for-security-studies/

www.instagram.com/css_jsia/

https://twitter.com/Css_Jsia

Important disclaimer

IB2211003

Introduction

Robert David Steele explains Open-Source Intelligence (OSINT) as "unclassified information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question".[1] Simply put, it is the accessible and relevant information from public sources. Though this information is vastly present on the internet, it is not necessarily freely available. Open-source information is available from a wide variety of sources and presented in a variety of formats. It can either be proprietary, subscription-based or information available solely upon request. The collection, processing, analysis, and timely distribution of this information to the end user plays a vital role in intelligence and security planning. It is however necessary for the information to be gathered lawfully only. For the purpose of intelligence, the gathering of open-source information means overt collection rather than a covert collection of information. Understanding this difference is essential. The covert domain of intelligence work is still the core of intelligence and agencies designated to the same are given rights for using such tools. The following can be considered to understand the difference between overt and covert intelligence (in terms of legality) a little better. Consider gathering and collecting any kind of information from a person or organisation's social media account to be open-source intelligence in an overt manner. On the other hand, consider an unapproved entry into the same account through a stolen or found password. This cannot be considered OSINT. However, open sources have always contributed and played a major role in covert action as well. For example, Imperial Japan employed Alexander von Siebold - a German agent, to influence foreign opinion in Tokyo's favour. He launched the journal 'Ostasien' (East Asia) in 1899 with the help of the Japanese authorities and contributed pro - Tokyo articles to the European media, and otherwise worked to shape views on Japan around the world. At the same time, he also monitored the media, submitting his "Baron von Sie-bold's Report on the Press" to inform the Japanese of foreign developments and opinions.[2] An essential subset of open-source information is called Grey Literature. The Interagency Grey Literature Working Group (IGLWG) defined the same as follows:

[1] Robert David Steele, Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007), 129
[2] Nihon Gaikoshi Jiten, Dictionary of Japanese Diplomatic History, (Tokyo: Yamakawa Shuppansha, 1992) 361

Grey literature, regardless of media, can include but is not limited to, research reports, technical reports, economic reports, trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, dissertations, and theses, trade literature, market surveys, and newsletters. This material cuts across scientific, political, socio-economic, and military disciplines.[3]

The OSINT Handbook published by the North Atlantic Treaty Organisation mentions four types of open information:[4]

- Open-Source Data (OSD): These are primary sources in the form of raw data including first-hand photographs, recordings, notes, etc.
- Open-Source Information (OSINF): These include books, news reports, articles and broadcasts which are filtered and edited secondary sources.
- Open-Source Intelligence (OSINT): This kind of information is something that is already processed and disseminated to the selected end-users. It is used for addressing a specific question or requirement.
- Validated OSINT (OSINT-V): Coming from a reliable source, this OSINT information is considered to be of the highest level of validity as it comes from a reliable source. In terms of security planning and intelligence, it is often a product of an all-source analysis. It tests open sources by comparing them with classified sources. For instance, a news article may claim that a particular bridge, that is vital for a specific military force - exists. Classified sources in such a case may either confirm or negate the existence of such a bridge.

Not all of these types of open-source information and intelligence are applied in real life for multiple reasons. A moral dilemma plays in the application and exploitation of these sources as they can include sensitive information that might prove harmful to an individual or organisation when used. Some sources can be both private and public at the same time, depending on their

[3] Definition provided by Mr. Bruce Fiene, Executive Secretary, STIC - Open Source Subcommittee in a memo dated 15 October 1994.
[4] NATO Open Source Intelligence Readers, February 2002

nature of use like blogs and comments. Leaked or unintentionally shared private information is a serious issue for OSINT information gatherers and frameworks.[5]

Intelligence drives decision-making. While executing operations in the domain of security planning across spectrums ranging from total war to humanitarian assistance, open-source intelligence systems provide a solid foundation for security planning and executing coalition operations. It also comes from the fact that intelligence has become transparent, relatively affordable, and faster since the detailed analysis of open information sources. To ensure maximum productivity, open-source intelligence systems shall not be competed with other intelligence patterns but instead be used in an all-source combination. Open-source intelligence systems are not a substitute for any existing organic and traditional military and civilian intelligence capabilities but a facilitator to these. Intelligence facilitates the use of open sources by all staff elements such as Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT) that require access to relevant, reliable information for different purposes. Figure 1 is the original graphic that captured Robert Steele's vision for leveraging Open-Source Information (OSIF) and Open Source Intelligence (OSINT) to dramatically improve the effectiveness of the classified disciplines and consequently the reach and insight of the all-source analysts[6]. For instance: In a HUMINT intelligence research cycle[7], open-source intelligence can help in mapping contacts and research areas for spotting relevant figures, assessing and evaluating individuals, checking people's claimed recollection against publicly available information sources, etc. Open-source intelligence systems not only provide factual information but also strategic and cultural insights. It sends out helpful information about infrastructure and current conditions and tactically vital commercial geospatial information that is not available from national capabilities. Thus, in the modern era, the OSINT product has become the answer to almost all intelligence needs.

[5] Potz, Tin, The Increasing Importance of OSINT as a Source of Intelligence, (University of Zagreb, 2021)
[6] Graphic: OSINT All-Source Temple - Public Intelligence Blog
[7] Intelligence cycle is a simplification of the intelligence-making process divided into 5 – 6 steps. It contains planning and direction, collection, analysis and production, dissemination, and feedback or requirements that start the process all over again (McGlynn and Garner, 2019: 13)

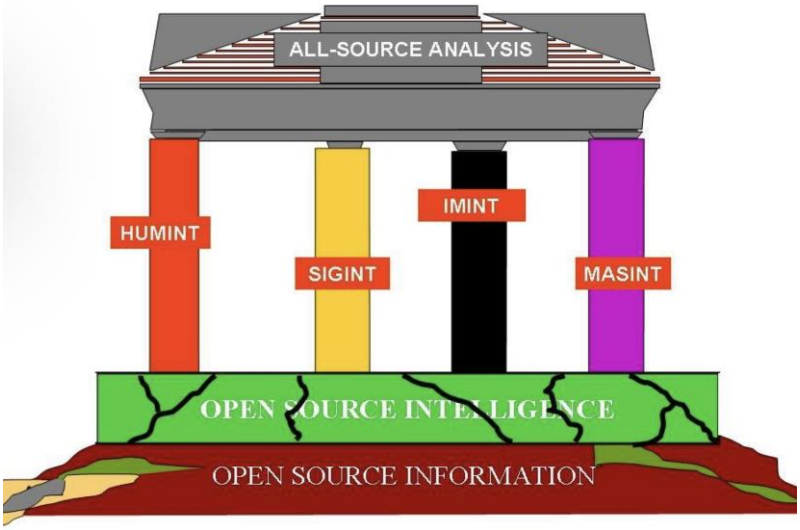

Figure 1 - OSINT as the foundation facilitating other intelligence frameworks, as explained by Robert Steeve[8]

Within the coalition operations context, OSINT provides a unique simultaneous approach. It provides a "multilateral foundation for establishing a common view of the shared Area of Operations (AOR), while also providing a context within which a wide variety of bi-lateral classified intelligence-sharing arrangements can be exploited."[9] Figure 2 explains this approach.[10] Providing information about the past, the present, and the future - open sources are relatively richer than closed resources. In 1969, Herman Croom highlighted the validity and importance of open-source information in an academic paper. The said paper is now a declassified CIA document. Here, he takes the example of nuclear programs, which can by no means stay invisible and discrete from the international eye. Reparations for such a program take many years and a lot of monetary resources. This information can be gathered by monitoring economic data, proving OSINTs value.[11] Apart from this, Croom also clarifies that in a situation where one is being flooded by fake

[8] Graphic: OSINT All-Source Temple - Public Intelligence Blog
[9] Robert David Steele, Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007)
[10] Robert David Steele, Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007), 130-132
[11] Hamilton Bean,No More Secrets: Open Source Information and the Shaping of US Intelligence, (Praeger Security International, 2011).

stories from the foreign media officially, the opposite side's real technological advancements can be noticed[12] fairly from their scientific, academic papers and in-house communications.

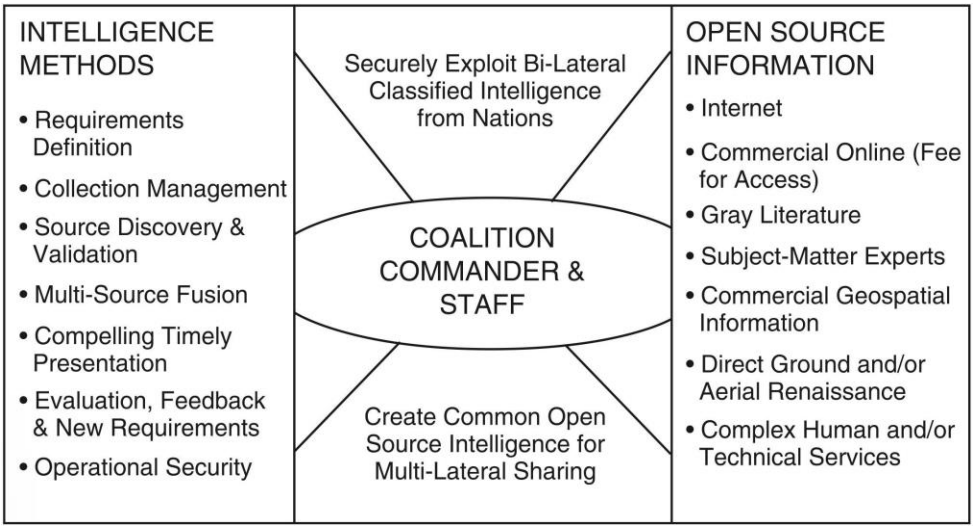

Figure 2[13] - Bi-lateral classified intelligence-sharing arrangements

History and Development of OSINT

'Open Secrets' during the Second World War

The real amalgamation of technology and intelligence happened during the Second World War. It acted as a catalyst for the development of open-source intelligence systems by giving the space to create the first-ever open-source analyses jobs and institutions for gathering open-source information. The earliest of such institutions - the Foreign Broadcast Monitoring Service (FBMS) was started by the planned methodological efforts of the United States' intelligence agency. It was responsible for collecting, filtering, transcribing, translating, and processing radio signals and broadcasts in selected countries. The information target was mainly the Axis power's propaganda.

[12] Potz, Tin, The Increasing Importance of OSINT as a Source of Intelligence, (University of Zagreb, 2021)
[13] Robert David Steele, Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007), 131

While the goals were kept transparent to the American citizens, FBMS was one of the few intelligence initiatives and institutions to be made public. In the 60s, its activity expanded to monitor all foreign media.[14] During the Second World War, not only the CIA but also the Office of Strategic Services, the wartime intelligence agency of the United States relied on open-source information and intelligence for security planning. The British Broadcasting Corporation (BBC) in 1939, launched a civilian which later developed into a commercial service to scrutinise foreign print journalism and radio broadcasting. This was introduced at the request of the British government. It was then known as the Digest of Foreign Broadcasts (now known as BBC Monitoring). As a British Broadcasting Corporation handbook from 1940 clarifies, the aim of the same was to build a "*modern Tower of Babel, where, with exemplary concentration, they listen to the voices of friend and foe alike*."[15]

By mid-1943 the BBC had started to monitor 1.25 million broadcast words daily. At the same time, agencies in the US were trying to improve their intelligence frameworks by using more and more open-source techniques.[16] In the late 1940s, a formal partnership between the BBC and its US counterpart was instituted, with an agreement to exchange all the output each of them received and full transparency of information. BBC Monitoring's key trademark is that it tells you "*the words as spoken*" - exactly what a television service is reporting, exactly what a minister says in an interview exactly what a treaty contains.[17] Even in 1941, during the Nazi invasion of the Soviet Union, open-source information (also understood as overt intelligence) obtained from the enemy and the neutral press was the only regular and reliable source of intelligence available to the British government from the entire Nazi-occupied Soviet Union. This also occurred as a result of the 1940 Foreign Office ban on all British covert intelligence and espionage activities.[18]

The significant role played by OSINT ('along with covert intelligence traditional espionage) during the Second World War is beyond question. The Joint Intelligence Committee (JIC) was overseeing the direction and working of Britain's wartime intelligence operations. In 1945, the leaders of the committee published a report. The report illustrated that "even in times of war, much

[14] Ibid.
[15] Florian Schaurer, and Jan Störger, Guide to the Study of Intelligence, (Journal of U.S. Intelligence Studies, Volume 19, 2012)
[16] Ibid.
[17] NATO Open Source Intelligence Readers, February 2002
[18] Ben Wheatley, British Intelligence and Hitler's Empire in the Soviet Union, 1941-1945 (Bloomsbury, 2018)

of the information which was of value to the Foreign Office and Defence Services was in no way a secret and that the 'foreign press' was one of the most 'principal' wartime intelligence channels." This was a significant statement that indicated the value and faith the JIC leadership had in OSINT during the Second World War.[19] Sir Harry Hinsley[20] further explored the evidence about the important role played by OSINT in the Second World War. He observed that out of the total number of reports received by the Enemy Branch of the Ministry of Economic Warfare, around three-fifths were based upon the Press, news coverings, broadcasts and official statements.[21]

'Finding Missing Pieces' during the Cold War

During this time, expensive spy satellites were the major source of finding out the number of intercontinental ballistic missiles the enemies had. At the same time, the role played by open-source intelligence and information was increasing. Intelligence officers and experts in open sources continued to help analysts and officials navigate the murky waters of the Cold War, even after the guns of the Second World War fell silent. By the time the Cold War started in its maximum glory, open sources and the techniques related to the framework had become well-established resources of information. As Joseph Nye validates it, they were "*the outer pieces of the jigsaw puzzles.*"[22] As the tensions of the Cold War elevated, the major countries on both ends of the Iron Curtain made sure to create and develop strong open-source collection capacities. These were often part of their clandestine intelligence services. According to Stephen Mercado, the Chief Analyst of the CIA, the open sources were serving beneficially in two ways. One, they were a 'major part' of all intelligence activities by that point in the war. Two, they were also the leading source of information about the opposition's military capabilities and political intentions, including early warning and threat forecasting[23]. It was therefore useful in security planning. If anything, OSINT had become relatively more efficient. The East German Ministry for State

[19] Michael Herman, The Post-War Organization of Intelligence, The January 1945 Report to the Joint Intelligence Committee on 'The Intelligence Machine' (Washington, Georgetown University Press, 2011) 38 - 41
[20] official post war historian of British Intelligence
[21] Frank Hinsley, British Intelligence in the Second World War, vol 2
[22] Committee on Homeland Security: Giving a Voice to Open Source Stakeholders, undated newsletter
[23] Mercado Stephen, Sailing the Sea of OSINT in the Information Age: A vulnerable source in the new era, CSI Publications, Studies in Intelligence, Vol.48 No. 3 (2004)

Security, (MfS, known as the "Stasi") for instance, analysed a thousand Western magazines and 100 books a month, while also summarising more than 100 newspapers and almost 12 hours of West German radio and TV broadcasting daily.[24] The western intelligence community, during the Cold War, had one adversary - the Soviet Union and its containment.[25]

It is important to note that the Western intelligence services majorly targeted the soviet – bloc economies, including that of the German Democratic Republic during the Cold War. A missing dimension in their policies and decisions towards the bloc is the economic intelligence aspect. The benefits of engaging in economic espionage and intelligence were all clear and straightforward.[26] This was important because the present (then) economic policies revealed the future intentions and analysis of the same would clarify the overall plans of the communist leaders. Moreover, it would also give a decent assessment of the future relative strengths of the Soviet bloc as compared to the Western world. The U.S. and their allied intelligence agencies relied on a different number of information sources, ranging widely from open-source information (OSINT) to HUMINT in form of spies, migrants, defectors, and travellers; to intercepted communications; and imagery intelligence from aerial and space photography (IMINT) in order to carry out this analysis. Not only was economic intelligence collected and analysed; much of it was published while the Cold War lasted.[27] The civilian economy of the regional bloc was extensively analysed as well. The US Central Intelligence Agency's findings about the Soviet economy were provided to the Joint Economic Committee (JEC) of the U.S. Congress for anthologies assessing the USSR's economic performance.[28] This led to the USA following an aggressive warfare economic policy in the late 1940s and early 1950s, the United States pursued an economic warfare policy that extended beyond an embargo on strategic trade. Such a policy was intended to weaken the Soviet economy and thus diminish the resources available to them to produce weapons and other arms. The intelligence reports from this period pinpoint vulnerabilities of the economies of the Soviet and East European that could be exploited. However, the intelligence reports from the late 1950s

[24] Florian Schaurer and Jan Störger, The Evolution of Open Source Intelligence (Journal of U.S. Intelligence Studies, 2012)
[25] Harris Minas, CAN THE OPEN SOURCE INTELLIGENCE EMERGE AS AN INDISPENSABLE DISCIPLINE FOR THE INTELLIGENCE COMMUNITY IN THE 21st CENTURY? (RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES, 2010)
[26] Minh A. Luong , Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007),
[27] Paul Maddrell, The Economic Dimension of Cold War Intelligence-Gathering, (Journal of Cold War Studies,, Vol. 15, No. 3, The MIT Press, 2013)
[28] Ibid.

indicated that the bloc economies were relatively self-sufficient and were not completely reliant on trade practices with the West nations. Hence, it was unlikely that denial of all trade would have a major impact on their economies. The Western European countries, in part for this reason, by 1954 (in the wake of Iosif Stalin's death) had succeeded in bringing an end to this multilateral economic warfare. Considering the same, around half of all items were removed from the list of embargoed goods by the United States. While the easing of the embargo was attributed mostly to the economic and political needs of the West European states - which is a fair argument - it was also driven partly by intelligence.[29]

'OSINT and New Security Challenges' post-Cold War

After the end of the Cold War in 1992, the Deputy Director of Central Intelligence, Admiral William O. Studeman reported on the contributions and capabilities of open sources during the ideological tussle of the world. His writing in the American Intelligence Journal shows how much the use of OSINT was relevant and provides a futuristic aspect to the use of such intelligence. He writes:

"*We have identified some 8,000 commercial databases - and the vast majority has potential intelligence value…. The explosion of open-source information is most apparent in the Commonwealth of Independent States (ed. The former Soviet Union), where today, there are some 1,700 newspapers that were not published three years ago. FBIS monitors over 3,500 publications in 55 foreign languages. And each day it collects a half a million words from its field offices around the world and another half a million words from independent contractors in the U.S. - that's equivalent to processing several copies of War and Peace every day.*"[30]

The revolution in information technology, commerce, and politics since the end of the Cold War has made pen sources more accessible, ubiquitous, and valuable. Simply put, one can gather more open intelligence information with greater ease and at less cost than ever before.

[29] Jackson, United Kingdom's leading role in narrowing the scope of the embargo, The Economic Cold War, 2011
[30] NATO Open Source Intelligence Readers, February 2002

Once the Soviet Union collapsed, western intelligence decided to redirect their energy and sources towards operations in new geographical and thematic regions with different priorities.

The intelligence spectrum of work and open-source data gathering expanded towards Asia and Africa mostly. Non-state actors, political and religious terrorism, the proliferation of weapons of mass destruction and the vulnerabilities of computer networks were also focused on.

It is clear that the use of OSINT and the needs that intelligence services need to meet in the modern world are different from the ones in the past. The new digital and public way of life brought greater possibilities for conducting OSINT. A large pool of primary information is created on the internet that can be processed by a computer and analysed by human analysts for insights.[31]Major technological developments in the Internet of Things (IoT) and big data[32] have boundlessly increased the amount of data and accelerated the advancement of open-source intelligence. The petabytes of data generated by social media represent the ideal context in which BDA can be used. Using open-source intelligence can help identify terrorist networks and provide valuable insights on other resources as well leading to a holistic intelligence approach. It also supports the identification of radical roots within the online community providing significantly increased capabilities and opportunities not just to prevent terrorist attacks, but to identify attack planning activity and most importantly, spot the early signs and signals of radicalisation and recruitment to stop violent and extremist development at source – this is a game-changer for counter-terrorism.[33] This also comes to light and gets a more serious approach (in importance) considering the failure of the American intelligence agencies to predict and get information about the 09/11 attacks well in time, when most of the information sharing and communication about the attack happened on the darknet in pro-jihadi and pro-al Qaeda group chats. The acquired data, when disseminated professionally, can be the basis for hacking financial crimes and virus spread. Moreover, it can also falsify data to give users inaccurate information or spread fake news to create confusion.[34] Thus increasing the instances of cyber-crimes including but not limited to hacking, data loss, denial

[31] Robert David Steele, Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007)
[32] Big Data is an evolving term that includes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information.
[33] Andrew Staniforth, Big Data and Open Source Intelligence- A game changer for counter terrorism. (Trends Research and Advisory)
[34] Ed.Yan Huo, Current Status and Security Trend of OSINT, (Hindawi Wireless Communications and Mobile Computing Volume 2022, Article ID 1290129)

of service attacks, spreading viruses, fake news and illegal use in various fields, such as gaming and financial shopping.[35]

In a recent development on similar lines, countries are now using the open-source framework and platform to maintain peace and security within their domestic territory. The June 2022 National Terrorism Advisory Bulletin of the Department of Homeland Security (USA) cites the recent mobilisation of threat actors and points towards the potential domestic violent extremists (DVEs) activities that would ramp up their calls for violence amid the U.S. mid-term election cycle.[36] As a part of domestic security planning, it is vital to combat such threats. Law enforcement agencies need to identify and monitor DVEs who are likely to act on their violent impulses while protecting Americans' right to free speech and protest. Fortunately, 90%-95% of the information that is being exchanged between these hostile actors is considered to be open source i.e. publicly available but primarily located below the surface on the deep and dark web.[37] In such cases, open-source intelligence tools and techniques can help agencies sift through huge volumes of data that often go unindexed, to uncover patterns and connections, and in turn alert agencies to threat actors that require closer attention than others.

Russia-Ukraine Conflict

On 24 February 2022, Russia invaded Ukraine which majorly escalated the Russia – Ukraine crisis. At present, both sides are engaged in a rhetorical and political conflict which is clear from direct and indirect military actions. They have not only tried to encourage their own populaces and forces in their favour but also have attempted to swat the international sentiment in their favour. This was done by both sides through numerous media attention tact tics. OSINT has played an important role not only on the battlefield in the region but also in other aspects. The applicability of OSINT during an international conflict spreads out in a wide spectrum ranging from Indications and Warnings (I&W) to humanitarian developments[38]. It, to a great extent, aids in the success of both sides. OSINT can be used for early warnings and predictions of possible regional conflicts. Take,

[35] Ibid. 34
[36] The bulletin is set to expire on November 30 2022 at 2:00PM ET
[37] September 1, 2022, Police1 by Lexipol blog
[38] Robert David Steele, Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007)

for instance, the big data landscape two months before Russia attacked. An analysis of intelligence and media attention proves that there was a noticeable rise in anti-Ukrainian sentiments accompanied by a sharp rise in daily social media posts that were pro-Russia. Over 500 separatist influencers posted unique content about Ukraine that accused it of being an aggressor, human rights violators, etc and the Russian media painted NATO as a strong aggressor. This was done in an attempt to create a pretext of invasion and to justify the Russian call for armed conflict. This campaign continued till February 2022 prior to the invasion. Disinformation like shelling and sabotage in the separatist republics; withdrawal of Russian troops; sabotage of a chemical plant; and the killing of Russians in the Donbas were being talked about.[39]

In recent years, OSINT has come to encompass an array of unclassified material available online or for purchase. According to the Defence Intelligence Agency, about 80%[40] of the intelligence information today comes from open–source material and unclassified sources. In the case of the current crisis, the Ukrainian give and the military were able to shape the war in their favour for a brief amount of time due to their ability to understand and decode the enormous amount of open-source information. Moreover, they are heavily investing in developing specialised analytical capabilities to extract information from open sources for a better war foot. OSINT has very efficiently assisted the Ukrainian military to track Russian military movements, plans, and operations. The most basic yet the most key piece of information comprises satellite images giving information on Russian target areas. Ukrainians have been able to eavesdrop on Russian communications and social media posts (both from Russian soldiers and Ukrainian citizens) due to open-source access to unencrypted radio waves and cell phone patterns. These updates on social media have been showing what a war ground looks like, giving Ukrainian officials insights into where and how the Russian military is operating. While Russia's military is stronger, larger, and more technically advanced, the advantages provided by OSINT have given the government of Ukraine a chance to challenge them.

The Russian officials have not unnoticed or ignored the impact of open-source information on their military goals. They have also made good use of open-source technology. In response, the Russian

[39] Richard Baffa, The Ukraine-Russia War Confirms the Value of OSINT, (Babel Street Blog)
[40] Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source' Data, as reported by The Wall Street Journal

government is pulling all strings to trap Ukraine under an umbrella of censorship. They have destroyed and disabled infrastructure in various places; estimates say that around 20% of telecommunications infrastructure in Ukraine has been damaged by the Russians.[41] In other cases, Russia is rerouting Ukrainian telecommunications infrastructure to go through Russian internet providers.[42] The Russian government has therefore been able to monitor emails, normal messages and all other forms of communication in order to curb the spread of open-source information.

Conclusion

While secrecy is embedded in the culture of the intelligence community, danger and exclusiveness over information have always been the main associates. Today, technology puts new data/information into circulation by the second. New technologies are deployed and regulated around the world on a daily basis.[43] As open sources are becoming accessible and affordable, the approach to security, in the modern world, is getting more and more complex. In the current technologically advanced environment, OSINT plays a crucial role in the security planning and threat landscape. By now, it is well established that open-source information when combined with covertly gathered information increases the value of final intelligence. In the context of traditional security, OSINT has time and again proved to be useful in strategic intelligence, and tactical intelligence in the form of detailed open–source maps. When it comes to traditional security, it can be used for contextual knowledge in expeditionary warfare, strategic intelligence, or tactical intelligence in the form of detailed open-source maps. However, global risks become less classical, and OSINT takes a contemporary approach. The Internet, for a relatively large amount of information, acts as the main source today. With the modernised way of living, the importance of OSINT has increased transferring its usage and function to the virtual realm. The importance of OSINT in today's intelligence has increased since the way of living has modernised and in part transferred into the virtual realm. The daily lives of ordinary citizens are being recorded at all times, to be used as sources of intelligence analysis later. Whether it was the sleep schedule of the army camps during the Second World War or the sighting of social media posts to track the

[41] Vanessa Smith Boyle, How OSINT Has Shaped the War in Ukraine, the American Security Project Journal
[42] Ibid.
[43] Ibid. 34

movement of the forces on the ground during the Russia-Ukraine war (as done through TikTok) - the smallest details can turn into important data. Web intelligence creates a pool of primary and secondary data/information. The solution to modern security problems, such as ecological disasters, migration, infectious diseases, or plain old terrorism, seems to lay in all-source analysis, also containing OSINT.[44] This has opened a wide window of opportunity for the intelligence community to use to its advantage. Here, creativity can be considered the specialty of OSINT. This is especially important when dealing with modern security threats, as creativity is the only solution for thinking of the unthinkable but dangerously probable.[45]

When it comes to intelligence technologies, India's domestic capability is sorely missing. To a great extent, India depends on Israel and the United States for its intelligence needs. With the privatisation and commercialisation of espionage, technology providers are going to be the biggest beneficiaries. If India continues to lag in this domain, it will become very difficult for it to become a smart power in the time frame it desires. A robust base in technology and innovation can strengthen national security, which in turn bolsters the economy.[46] Rapid experimentation in the field is the need of the hour. There is still a lot to discover, and OSINT can prove to play a dynamic role in the intelligence needs of the fast-developing 21st century. If the government gives proper attention to open-source intelligence and information and attracts the proper, it can benefit on various spectrums lauding the non-governmental and private organisations. The indispensable role of OSINT will become more evident than ever.

[44] Ashwell, Lawrence, The digital transformation of intelligence analysis (Journal of Financial Crime, 2017) 24
[45] Potz, Tin, The Increasing Importance of OSINT as a Source of Intelligence, (University of Zagreb, 2021)
[46] Dalmia, Kapoor, Datta, India's Enduring Challenge of Intelligence Reforms, (ORF Issue Brief, No. 428, December 2020)

Bibliography

Andrew Staniforth, Big Data and Open Source Intelligence- A game changer for counter terrorism. (Trends Research and Advisory).

Ashwell, Lawrence, The digital transformation of intelligence analysis (Journal of Financial Crime, 2017) 24

Ben Wheatley, British Intelligence and Hitler's Empire in the Soviet Union, 1941-1945 (Bloomsbury, 2018).

Committee on Homeland Security: Giving a Voice to Open Source Stakeholders, undated newsletter.

Dalmia, Kapoor, Datta, India's Enduring Challenge of Intelligence Reforms, (ORF Issue Brief, No. 428, December 2020)

Ed.Yan Huo, Current Status and Security Trend of OSINT, (Hindawi Wireless Communications and Mobile Computing Volume 2022, Article ID 1290129).

Florian Schaurer, and Jan Störger, Guide to the Study of Intelligence, (Journal of U.S. Intelligence Studies, Volume 19, 2012)

Frank Hinsley, British Intelligence in the Second World War, vol 2.

Hamilton Bean,No More Secrets: Open Source Information and the Shaping of US Intelligence, (Praeger Security International, 2011).

Harris Minas, CAN THE OPEN SOURCE INTELLIGENCE EMERGE AS AN INDISPENSABLE DISCIPLINE FOR THE INTELLIGENCE COMMUNITY IN THE 21st CENTURY? (RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES, 2010)

Jackson, United Kingdom's leading role in narrowing the scope of the embargo, The Economic Cold War, 2011

Mercado Stephen, Sailing the Sea of OSINT in the Information Age: A vulnerable source in the new era, CSI Publications, Studies in Intelligence, Vol.48 No. 3 (2004)

Michael Herman, The Post-War Organization of Intelligence, The January 1945 Report to the Joint Intelligence Committee on 'The Intelligence Machine' (Washington, Georgetown University Press, 2011) 38 – 41.

Minh A. Luong , Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007).

NATO Open Source Intelligence Readers, February 2002

Nihon Gaikoshi Jiten, Dictionary of Japanese Diplomatic History, (Tokyo: Yamakawa Shuppansha, 1992) 361.

Paul Maddrell, The Economic Dimension of Cold War Intelligence-Gathering, (Journal of Cold War Studies,, Vol. 15, No. 3, The MIT Press, 2013).

Potz, Tin, The Increasing Importance of OSINT as a Source of Intelligence, (University of Zagreb, 2021)

Robert David Steele, Ed, Loch K. Johnson, Handbook of Intelligence Studies, (New York, Routledge, 2007)

Vanessa Smith Boyle, How OSINT Has Shaped the War in Ukraine, the American Security Project Journal