CENJOWS

ISSUE BRIEF

# FROM CIVILIAN SLEUTHS TO MILITARY STRATEGY: ROLE OF OSINT IN THE RUSSIA-UKRAINE WAR AND LESSONS FOR INDIA

EMMANUEL SELVA ROYEN

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future ★ Victory through Joint Knowledge

CENJOWS

# FROM CIVILIAN SLEUTHS TO MILITARY STRATEGY: ROLE OF OSINT IN THE RUSSIA-UKRAINE WAR AND LESSONS FOR INDIA

**Emmanuel Selva Royen,** is a Research Intern at CENJOWS, New Delhi

## ABSTRACT

The Russia-Ukraine War is considered to be an inflection point in the method of warfare. The domain of intelligence in warfare has evolved significantly, with characteristics such as the increasing role of civilians in the kill chain, revolution and increased accessibility of technology and democratisation of Intelligence Surveillance and Reconnaissance. This is essentially because of the exponential increase in the information available to the public. In this context, it is important to understand and examine these developments to assess their implications for international and national security. Drawing to this, the paper has briefly traced the evolution of intelligence using open sources, and the extent to which OSINT can be used in ISR operations. Using the Russia-Ukraine War as a case, the paper has examined and drawn lessons for India's national security in the context of intelligence in the information operation context.

***Keywords:*** *Russia-Ukraine War, Open Source Intelligence, Intelligence, Surveillance and Reconnaissance, Intelligence Fusion*

## INTRODUCTION

Throughout the annals of history, the conduct of war between nations has borne witness to a relentless evolution of technology and strategic acumen. In pursuit of advancing their capabilities against enemy states, nations have driven the conduct of warfare to new frontiers. A pivotal milestone in this trajectory was the inception of military internet in 1969, not long into the Cold War, conceived by the U.S. as a military endeavour to share information with a network of government agencies and defence attaches.

Similarly, like how every war has brought an evolution in technology, the Russia-Ukraine war, the first state vs state conventional war in the Twenty first century which involved a major military power, witnessed a revolution in how warfare is conducted in every aspect. [1] Especially so in the domain of intelligence. No longer confined solely to nation-states, Intelligence in the Russia-Ukraine war has cast a wide net, ensnaring civilians as active participants. States are not the only producers and consumers of Intelligence anymore, with civilians stepping forth as agents in monitoring, gathering, and analysing publicly available information, into intelligence at the operational and tactical levels.

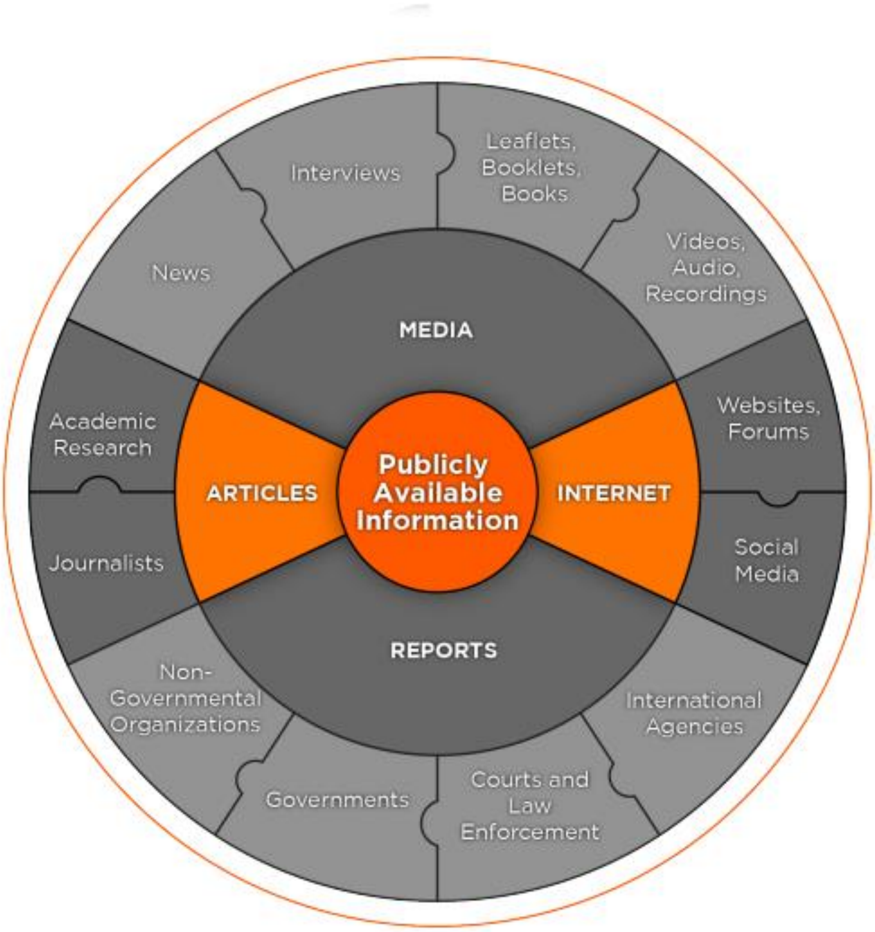
Interviews
Leaflets, Booklets, Books
News
Videos, Audio, Recordings
MEDIA
Academic Research
Websites, Forums
ARTICLES
Publicly Available Information
INTERNET
Journalists
Social Media
REPORTS
Non-Governmental Organizations
International Agencies
Governments
Courts and Law Enforcement

**Fig.1 Publicly Available Information Data Sources** (Greiger, Corrine. 2022. “The Reawakening of Open-Source Intelligence.” *MI Professional Bulletin* 34, no. 22 (April): 9-12.)

[1] “Ukrainians are changing approaches to modern warfare. Here is how.” 2023. Russia's war in Ukraine. https://war.ukraine.ua/articles/ukrainian-innovations-are-changing-approaches-to-modern-warfare/.

This practice of collecting, decoding and analysing Publically Available Intelligence (PAI) to provide intelligence is Open Source Intelligence (OSINT). This aligns with the US congress definition of OSINT as “intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.”[2] Publicly available information (PAI) is broadly referred to as "information that has been published or broadcast for public consumption, is available to the public upon request, is accessible to the public online or in another way, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any location or attending any event that is open to the public."[3] Fig.1 comprehensively depicts the various sources of (PAI).

Open Source Information is simply unclassified, publicly available data, while OSINT results from applying processing and exploiting the information to validate it as relevant, accurate, and actionable for use by the consumers.

During the Russian buildup on its western borders, Civilians equipped with smartphones have recorded and disseminated the movements of troops and machinery. In addition, private satellite companies have offered a comprehensive array of intelligence assets, encompassing optical and Synthetic Aperture Radar (SAR) images, alongside other sensor-collected data pertaining to specific areas of interest in the conflict zones. This valuable information is disseminated freely across social media and website platforms operated by said companies.

A group of civilian OSINT hobbyists around the world have assumed the role of investigators, diligently monitoring this PAI and making sense of it. This process, on occasion, culminates in the transformation of raw data into actionable intelligence for potential adversaries. However, this involvement on the part of civilians entails a notable element of jeopardy. Should this intelligence dissemination pose a threat to the hostile State, the civilian agents become inextricably linked to the adversary's kill chain, making them susceptible to targeting.

In this context, the issue brief will first look into the evolution of OSINT, and how it is used in Intelligence Surveillance Reconnaissance (ISR) capabilities. Second, the role of OSINT in the Russia-Ukraine war is examined in three layers of intelligence; Strategic, Operational and Tactical. Finally, with the above examination, lessons are drawn and recommendations are provided for India in its information operations considering its security environment.

[2] 109th Congress. 2005. “SEC. 931. DEPARTMENT OF DEFENSE STRATEGY FOR OPEN-SOURCE INTELLIGENCE,” [excerpt on open source intelligence; as reported by the House Armed Services Committee].

[3] Greiger, Corrine. 2022. “The Reawakening of Open-Source Intelligence.” MI Professional Bulletin 34, no. 22 (April): 9-12.

## OSINT IN ISR OPERATIONS: CONVENIENCE AND CREDIBILITY

### Evolution of OSINT: First and Second Generation OSINT

OSINT's inception came from a military intelligence initiative. The US formed the Foreign Broadcast Monitoring Service in 1941, later renamed as Foreign Broadcast Information Service (FBIS) and transferred to the CIA from the War Department in 1947.

The purpose of FBIS was to produce "open source intelligence," reports for the US government. It listened to foreign radio broadcasts and tried to analyse their news and sentiments against other states. The FBIS provided critical insights for the military entities during the Cold War, including the early indications of removal of cruise missiles from Cuba, the Soviet withdrawal from Afghanistan, and the crisis in the Balkan states. Around eighty per cent of the intelligence to monitor the collapse of the Soviet Union came from open sources.[4]

Therefore, the first generation OSINT is based on the collection of news updates and other development briefings of foreign states through broadcasting and print media, which may be used in aiding the foreign policy of a country.

The second generation of OSINT, has evolved from the rise of social media and Web 2.0 in 2005. OSINT in the second generation is based on virtual accessibility, constant acquisition and exploitation. While the first generation exploited audio and textual information, the second generation OSINT tries to exploit all types of media simultaneously from audio, video and images.[5]

The Russia-Ukraine war may again be a point of inflection in the evolution of OSINT. The emergence of third-generation OSINT is heavily influenced by several key aspects, including the exponential growth of information, its collection, and processing.[6] The scope of OSINT has expanded beyond just visual digital media to include radar and signals intelligence, which are gradually becoming publicly accessible. [7] With an increasing number of sensors involved, optical lenses are no longer the sole source of data. In fact, a typical smartphone alone is equipped with approximately 12 sensors that provide data on position, proximity, elevation, and

4[] Mercado, Stephen. 2004. "Sailing the Sea of OSINT in the Information Age." Studies in Intelligence 48 (3): 45-55.

5[] Williams, Heather J., and Ilana Blum. 2018. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. N.p.: RAND Corporation.

6

[] Vandersmith, Midshipman First Class Owen. 2023. "How Open-Source Intelligence Is Changing Warfare." The Naval Review 149, no. 3 (March): 1441.

7

[] Weinbaum, Cortney, Steven Berner, and Bruce McClintock. 2017. "SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain | RAND." RAND Corporation. https://www.rand.org/pubs/perspectives/PE273.html.

environmental changes. These data can be easily shared online, either in visual form or through underlying metadata formats.

The integration of new and emerging technologies such as Artificial Intelligence (AI) and Machine Learning has further accelerated the processing and analysis of vast volumes of information sourced from various sensors. These technologies play a crucial role in handling the enormous influx of data, making it feasible to extract valuable insights and patterns in a timely and efficient manner.

As conflicts and geopolitical situations evolve, OSINT continues to adapt and refine its methodologies to keep pace with the challenges presented by the ever-increasing amount of data generated by diverse sources.

## OSINT in ISR Operations

ISR operations provide a state with the intelligence necessary to identify and assess potential threats to its national security. This includes tracking the activities and capabilities of other states, non-state actors, and terrorist groups that may pose a risk to the country. ISR is critical for military operations as it provides commanders with real-time information about the battlefield, including the location of friendly and enemy forces and the movements of critical assets such as tanks, aircraft, and ships. This information enables commanders to make quick and accurate decisions, which can be the difference between success and failure in modern warfare.

Traditionally, ISR operations were only performed by nation-states largely because of the resources owned by it. However, satellite images, radio frequencies detection, and real time images are now publicly available. Satellite service companies like Maxar and Black Sky provide optical and radar images of conflict zones. Ship vessels and aeroplanes can also be tracked using their mandated open Automatic Identification System (AIS). There are OSINT hobbyists who monitor and detect unusual flight or vessel movements in areas of interest. Therefore, the reliability and acceptance of OSINT by the State's defence in their ISR needs to be assessed.

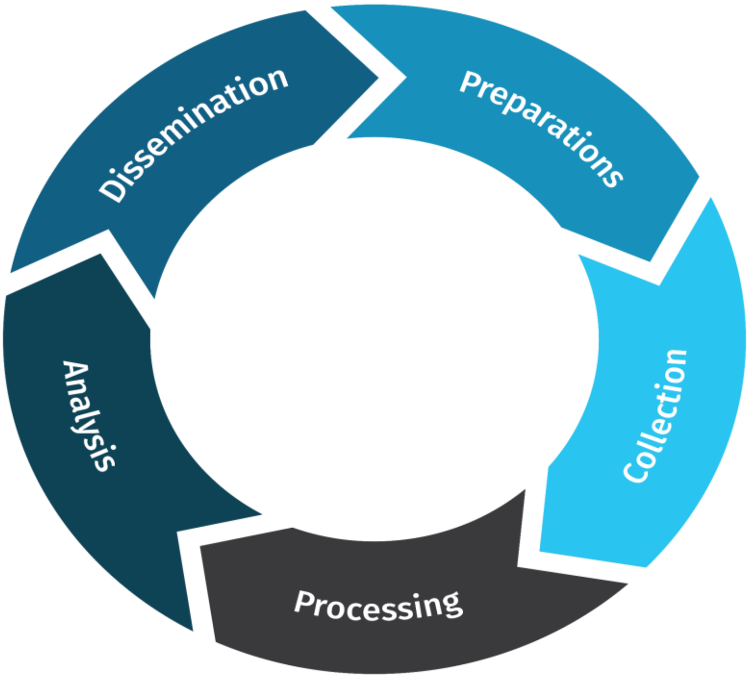

**Fig.2 What is OSINT (Open-Source Intelligence?**
(Gill, Ritu. 2023. “What is OSINT (Open-Source Intelligence?).” SANS Institute. https://www.sans.org/blog/what-is-open-source-intelligence/.)

The assessment of Open Source Intelligence (OSINT) can be effectively conducted by using the Intelligence Cycle, which encompasses various essential stages, namely Preparation, Collection, Processing, Analysis, and Dissemination (Fig 1).

During the Preparation stage, an in-depth evaluation of the information needs and requirements of the investigative request is conducted. This involves delineating the specific goals of the task and strategically selecting the most suitable resources to obtain the necessary data. In conventional intelligence practices, this process often involves utilising aerial reconnaissance for visual information and employing Human Intelligence (HUMINT) sources for real-time situational intelligence. Such conventional approaches, however, typically demand substantial resources and time to deploy assets for data collection. On the contrary, the OSINT methodology capitalises on the readily available public information, thereby enabling investigators to solely focus on identifying the pertinent information and selecting appropriate tools to extract it.

For instance, in scenarios where insights into the emotions of an area anticipating an influx of military troops are required, a sentiment analysis of social media posts can be conducted. Consequently, the OSINT approach allows for streamlined identification and procurement of the necessary requirements, tools, and subjects of interest with significantly reduced resource expenditure and time consumption.

The collection of data constitutes a pivotal and crucial stage within the Intelligence Cycle. Sherman Kent defines collection as “the surveillance operation” by which an area of interest or a target “is put under close and systematic observation”.

When the state undertakes data collection, it deploys its valuable and costly assets, comprising both human resources and advanced technology, on the ground. This pursuit exposes the state to significant risks, and the imperative to operate covertly further restricts the acquisition of information. In contrast, OSINT collection involves the compilation of publicly accessible data from diverse sources, including social media platforms, news articles, official records, academic journals, and business databases. This process can be carried out either manually by examining and scrutinising the sources or automatically by employing specialised programs capable of searching and aggregating data. Additionally, private companies such as Maxar and Space Nets have emerged as key contributors, providing valuable information related to areas of interest. This trend represents a noteworthy development within the intelligence community.

However, it is important to acknowledge that OSINT faces a significant challenge known as "event barraging," wherein social media platforms become inundated with a series of embellished or fabricated events that manipulate real-time occurrences.[8] This phenomenon can complicate decision-making processes during the tactical stage.

During the Processing stage, the collected information undergoes rigorous filtering, systematic organisation, and collation. The raw data extracted from various sources is integrated into a cohesive structure and timeline. In traditional intelligence practices, this integration necessitates the fusion of information from diverse sources and formats. However, with OSINT, as all data is extracted through computer-based means, it can be seamlessly consolidated within a single digital platform, such as a repository or a Geographic Information System (GIS), for further analysis in the subsequent stages. Challenges arising from event barraging can be addressed during this stage by corroborating OSINT with intelligence obtained from alternative sources.

In the Analysis and Production stage of the Intelligence Cycle, the collected and fused information undergoes comprehensive examination and interpretation to make it relevant for employment at the tactical level. During this stage, analysts identify patterns, track targets, determine their locations, and predict their future trajectories.[9]The insights derived from the analysis are then utilised to generate reports that address specific questions, draw conclusions, and propose further measures. In the context of OSINT, specialised techniques such as geolocation, satellite image analysis, and meta data analysis can be efficiently employed and integrated using the same processing platforms.

In the Dissemination stage, the final one, the intelligence gleaned from the analysis is provided to relevant stakeholders. This process is considerably faster compared to

[8] Rasak, Capt. Michael J. 2021. “Event Barraging and the Death of Tactical Level Open-Source Intelligence.” Military Review, (January), 48-57.

[9] Ziółkowska, Agata. 2018. “Open source intelligence (OSINT) as an element of military recon.” Security and Defence Quaterly 19, no. 2 (February): 65-77. https://doi.org/10.5604/01.3001.0012.1474.

traditional methods. OSINT analysis has the versatility to contribute to intelligence at various levels, from strategic decision-making to tactical planning, and can cater to both push and pull intelligence delivery. It is important to note that OSINT does not replace conventional state-owned ISR operations, but rather complements them. Integrating OSINT alongside existing ISR capabilities should be considered.

However, it is observed that defence personnel exhibit a bias against OSINT due to historical reliance on classified and clandestine intelligence to gain an advantage over adversaries.[10] Nevertheless, it is crucial to recognise that leveraging OSINT can provide significant advantages in terms of rapid data acquisition and insight generation, particularly in time-sensitive situations. Moreover, OSINT is a passive method of intelligence collection, which means the state's involvement with or proximity to the target is indirect, unlike operations involving secret agents.

To further substantiate the case for the use of OSINT in ISR operations during conflicts, the ongoing Russia-Ukraine War can be assessed and examined.

## OSINT IN THE RUSSIA-UKRAINE WAR

The employment of OSINT has played a significant role in the ongoing Russia-Ukraine War, involving participation from civilians, military personnel, and state intelligence agencies in the collection and analysis of publicly available sources. Notably, social media platforms and messaging applications have emerged as prominent avenues for civilians on the ground to report incidents and share media files related to the conflict. Local police forces and administrators have also leveraged platforms like Telegram to disseminate alerts and announcements within the conflict zone. As some social media platforms such as Twitter and Facebook are being subjected to sanctions by Russia, the country has resorted to its own social media application, VKontakte. On the other hand, Ukraine has employed a comprehensive range of social media applications, including both Western and Russian platforms. The use of OSINT in the context of the Russia-Ukraine War can be systematically analysed within the framework of the three intelligence levels: Strategic, Operational, and Tactical Intelligence.

### OSINT for Strategic Intelligence

Strategic intelligence (STRATINT) caters to support long-term decision making and planning at the national level with military interaction. It looks into understanding the larger geopolitical, economic, social and technological trends and developments that may impact national security. STRATINT provides a comprehensive and forward-looking perspective on potential challenges, risks and opportunities that lie ahead.

[10][] Weinbaum, Cortney, John V. Parachini, and JD Williams. 2021. “The Intelligence Community's Deadly Bias Toward Classified Sources.” RAND Corporation. https://www.rand.org/blog/2021/04/the-intelligence-communitys-deadly-bias-toward-classified.html.

Specifically, analysing Russia's ideology and President Putin's speeches could have provided clues about the country's strategic objectives and priorities. An examination of its military budget increase may have indicated the country's readiness for military action and potential aggressive posturing.

Additionally, conducting sentiment analysis of the people of Donbas would have offered valuable insights into the local population's attitudes and feelings, potentially highlighting simmering tensions or dissatisfaction that could be exploited or escalated by external forces.

Furthermore, a politico-psychology analysis of leaders like President Putin and President Zelensky might have shed light on their decision-making processes, personal biases, and possible responses to perceived threats or provocations.

The failure of Russia's STRATINT, as argued by numerous analysts, can be attributed to its inability to adapt to intelligence trends. Instead of leveraging a diverse and dynamic information ecosystem, Russia may have continued to rely on a constrained approach to intelligence gathering and decision-making typical of autocratic regimes.[11] This rigidity and resistance to change may have hindered their ability to accurately perceive and respond to the changing geopolitical landscape and potential risks posed by their actions

In February 2022, the political leadership in Russia made a serious error in estimating the internal political climate in Ukraine. Russian intelligence failures turned an attempted regime-change operation into a prolonged regional war of attrition, with its political objectives difficult to achieve and its military and economy both deteriorated by the conflict. This is in contrast to its accurate reading of the ground-level Ukrainian political ecosystem in 2014. Russian analysts speculated that the western nation-states would not respond to its actions as they were at their weakest point post-pandemic and were increasingly dependent on Russia’s oil and gas. However, Europe and the US emerged to provide funds and arms to Ukraine despite recession and the energy diplomacy of Moscow did not influence to limit Europe’s response. The failure of Russian analysts to employ political-psychology analysis of key western stakeholders like President Joe Biden and NATO secretary Jens Stolenberg led to further expansion of NATO towards the East.

A comprehensive STRATINT analysis incorporating various analytical methods, such as content analysis, sentiment analysis, and politico-psychology analysis, could have provided a more informed and nuanced understanding of Russia's intentions and

[11][] Dylan, Huw, David V. Gioe, and Elena Grossfield. 2022. “The autocrat’s intelligence paradox: Vladimir Putin’s (mis)management of Russian strategic assessment in the Ukraine War.” The British Journal of Politics and International Relations 25 (3). https://doi.org/10.1177/13691481221146113.

potential actions, potentially leading to better anticipation and prevention of the invasion of Ukraine.[12]

### OSINT for Operational Intelligence

Operational intelligence is to understand the adversaries' entities and potential battlespaces for the purpose of planning and conducting campaigns and operations. At the operational level, intelligence supports the planning and execution of the planning. While the planning stage is analytical, the support to the operation is driven by intelligence collection.[13] Intelligence preparation in an operational environment consists of evaluating the geographic terrain, adversaries capabilities and intent. Assessing the morale of adversaries soldiers and its own is also an important step.

During the initial stages of the Russian invasion, the military buildup was spotted and posted in the media by numerous civilians. Satellite imagery also confirmed the same, and private investigative companies and OSINT hobbyists already warned of Russia's invasion of Ukraine. The Kremlin, ignoring the presence of civilian's handheld sensors, lost their element of surprise in the offensive. Further when the Russian tanks marched into the Donbas region, they came to a halt due to fuel shortage. [14] Images and videos of this made them as sitting ducks for Ukrainian artillery and missiles. Moreover, Russia's inability to assess the morale of their soldiers led to the abandonment of numerous tanks in the conflict. The Russian forces were unable to employ OSINT to update their operational intelligence capacity and adapt and amend their plans to the dynamics on the field.[15] [16]

However, on the other hand Ukraine received operational intelligence from its Western allies and the willingness to use OSINT. Realising the potential of OSINT and the citizens with smartphones, Ukraine launched the app, Diia, which allows its people to post geotagged pictures and videos of Russian troop movements. The Diia app which was initially an e-document and identification platform for citizens at checkpoints was turned into a platform for reporting the movement of enemy troops. The US based space company Starlink, provided the internet needed in the areas where physical

[12] Waller, Jullian. 2023. "Intelligence Failures and Political Misjudgment in an Age of Ideological Change." The Strategy Bridge. https://thestrategybridge.org/the-bridge/2023/6/14/intelligence-failures-and-political-misjudgment-in-an-age-of-ideological-change.

[13] Abdalla, Neveen S., Philip H. Davies, Kristian Gustafson, Dan Lomas, and Steven Wagner. 2022. "Intelligence and the War in Ukraine: Part 1." War on the Rocks. https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/.

[14] BBC News. 2022. "Ukraine conflict: Why is Russia losing so many tanks?" BBC, April 11, 2022. https://www.bbc.com/news/world-61021388.

[15] Davies, Philip H. 2022. "No War for Old Spies: Putin, the Kremlin and Intelligence." RUSI. https://rusi.org/explore-our-research/publications/commentary/no-war-old-spies-putin-kremlin-and-intelligence.

[16] Mitzer, Stijn. 2022. "Attack On Europe: Documenting Russian Equipment Losses During The Russian Invasion Of Ukraine." Oryx. https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html.

infrastructure was destroyed. For a comprehensive and real-time view of operations, operational intelligence often integrates data from various diverse sources, both internal and external to the organisation. Ukraine was able to achieve this by fusing civilian provided information, friendly state's foreign intelligence and industry partnerships.

A statement from the White House stated that the US government is providing real time intelligence and details about the commanders of the Russian battalions. The UK Defence ministry also posts its daily intelligence brief of Ukraine on social media.

In the Air and Maritime domain, OSINT investigators from around the world have been closely monitoring unusual flight and vessel movements through open sources of signals intelligence.[17] During the Wagner rebellion, OSINt investigators spotted the president's plane leaving from the Kremlin. The dissemination of this news may have led to a significant psychological effect on the national guards of the Kremlin and soldiers on the battlefield. Russian naval ships have also been constantly monitored by the global intelligence community using Automatic Identification System (AIS) and Radio Frequency detectors to detect unusual manoeuvres and conflicts with other foreign naval ships in the Mediterranean Sea.[18]

Use of OSINT has also aided in bringing accountability and degrading a chance for plausible deniability and exposition of War Crimes. An NGO of Ukrainian Human rights defenders, Truth Hounds use OSINT to conduct investigations into war crimes. They established a database with distinct areas for suspected offenders and victims/survivors to register and share all cases of amassed war crimes.[19] The methodology was to connect instances that have the same patterns, such as the same perpetrators, time, area, scale, and operating mode, by structuring and fully developing each case. Cross-cutting this data enables the identification of some patterns associated with war crimes.[20] The utilisation of satellite imagery and geospatial

[17] Benjamin, Alec. 2023. "The importance of OSINT in the air war in Ukraine." OSINT for Ukraine. https://www.osintforukraine.com/publications/the-importance-of-osint-in-the-air-war-in-ukraine.

[18] Andre, Dave. 2017. "Seeing the Forest Through the Trees: The Value of OSINT for the U.S. Navy | Center for International Maritime Security." Cimsec. https://cimsec.org/seeing-forest-trees-value-osint-u-s-navy/.

Sutton, HI. 2022. "Covert Shores." H I Sutton - Covert Shores. http://www.hisutton.com/Russia-Med-BS-2022-02-15.html.; "track aircraft live." n.d. track aircraft live. Accessed July 20, 2023. https://globe.adsbexchange.com/.

[19] Amos, Deb. 2022. "Open source intelligence methods are being used to investigate war crimes in Ukraine." NPR, June 12, 2022. https://www.npr.org/2022/06/12/1104460678/open-source-intelligence-methods-are-being-used-to-investigate-war-crimes-in-ukr.

[20] Bergengruen, Vera. 2022. "How Ukraine Is Crowdsourcing Digital Evidence of War Crimes." Time. https://time.com/6166781/ukraine-crowdsourcing-war-crimes/.; Carrée, Lila. 2023. "The Role Of Technology In The Exposition Of War Crimes In Ukraine: How The Use Of Cutting-Edge Technologies And Open-Sources Investigations Can Expose Human Rights Violations." LSE Blogs. https://blogs.lse.ac.uk/humanrights/2023/02/02/the-role-of-technology-in-the-exposition-of-war-crimes-in-ukraine-how-the-use-of-cutting-edge-technologies-and-open-sources-investigations-can-expose-human-rights-violations/.

intelligence accessible in the public domain plays a significant role in evaluating the extent of damage inflicted on fertile farmlands during the conflict and in forecasting potential risks to food security.

The Kyiv School of Economics (KSE) Institute, in conjunction with the Government of Ukraine, spearheads an initiative known as "Russia will pay/damage.in.ua." This initiative serves as a comprehensive platform for gathering, assessing, analysing, and disseminating data pertaining to the impact of the Russian invasion on civilian infrastructure. Data is sourced from various channels, including government agencies, local authorities, residents, and other relevant sources. The primary objective of this endeavour is to estimate and continuously monitor the costs of war, effectively making it an open-source data initiative.

Through the collaborative efforts of this initiative, the assessment of damages to essential farmlands and civilian infrastructure provides valuable insights into the consequences of the conflict, contributing to a comprehensive understanding of its implications on food security and the overall well-being of affected communities. The transparent and publicly accessible nature of the data empowers researchers, policymakers, and concerned stakeholders to make informed decisions and respond effectively to the challenges posed by the conflict's aftermath

## OSINT for Tactical Intelligence

Tactical intelligence encompasses the prompt and focused gathering and examination of events at the operational level. Actionable intelligence derived from this process is selectively disseminated solely to commanders and frontline personnel during engagements. Due to its time-critical nature, TACINT necessitates swift collection, processing, and delivery, especially in dynamic situations. TACINT enhances situational awareness for commanders and field personnel. It provides them with a clear understanding of the battlefield or operational environment, including enemy positions, and threats.[21] The seamless integration of tactical intelligence with ongoing operations is integral, as it serves to inform decision-making on the ground, providing crucial guidance for tactics and responses during engagements.

When Russian soldiers on the battlefield posted videos and photos of them expressing discontent, Molfar, a Ukrainian private military intelligence company scrapped media posted by Russian soldiers on Vkontate and identified their location either through geolocation or metadata analysis. [22] They then provided the intelligence to Ukraine’s

[21] Ziółkowska, Agata. 2018. “Open source intelligence (OSINT) as an element of military recon.” Security and Defence Quaterly 19, no. 2 (February): 65-77. https://doi.org/10.5604/01.3001.0012.1474.

[22] Hewson, Jack. 2023. “A Private Company Is Using Social Media to Track Down Russian Soldiers.” Foreign Policy. https://foreignpolicy.com/2023/03/02/ukraine-russia-war-military-social-media-osint-open-source-intelligence/.

intelligence service Sluzhba Bezpeky Ukrainy (SBU), who then with further analyses confirmed the location and directed the artillery accordingly. [23]

Ukraine's Center for Innovation and Development of Defense Technologies of the Ministry of Defence of Ukraine and Aerorozvidka, invented an advanced digital map, Delta, which provides detailed pictures of specific areas of the frontline, allowing the soldiers to identify friend or foe. The ministry of digital transformation developed eVorog, a chatbot that allows civilians to report on the enemy troops, their movement and location.

Tactical intelligence also includes in emergency response situations, which involves providing critical information about the incident, such as the location of casualties or hazardous materials, to first responders for effective crisis management. During the initial months of Russian invasion, the battle in the Zaporizhzhia nuclear plant was a critical situation for the security of Europe. A four hour grainy security footage was released on the internet, and OSINT analysts were able to assess the situation of damages and safety of the plant.

## LESSONS FOR INDIA

From the above assessment and examination, and understanding the significance of OSINT in levels of intelligence during conflicts. Lessons for India can be drawn from it. At the outset, it is also important to understand India's security environment in the Information Operation context and India's intelligence culture to employ the lessons accordingly.

### India's Security Environment In the Information Operation Context

India has two hostile neighbours, Pakistan and China. Pakistan lacks behind India in ISR capabilities, therefore tends to use hybrid methods of conflict like Information warfare (IW). Pakistan's IW strategy primarily focuses on disinformation and espionage using social media. When the Indian Aiforce shot down Pakistan's F16 aircraft with MiG 21 Bison fighters during Operation Bandar on 26 February 2019, the Pakistan's Armed Forces media wing, Inter-State Public Relations (ISPR), denied this incident. This garnered support by a famous US based publication- Foreign Policy. However, after investigation of the aircraft debris, a missile part which was exclusive to fit F-16 was found. Pakistan employs disinformation tactics during any domestic issues in India to manipulate the people and grow animosity within. Pakistan's intelligence service is infamously known for its espionage through honey trapping Indian persons of interest.

China poses a difficult threat to India, as it has been constantly evolving its IW tactics and capabilities. For instance, during the Galwan Clash, adverse political opinion was garnered in India against the government about the negligence of armed forces. Chinese media also released videos of Indian army badly hurt by clubs embedded with

[23][] Browne, Malachy. 2022. "Caught on Camera, Traced by Phone: The Russian Military Unit That Killed Dozens in Bucha." The New York Times, December 22, 2022. https://www.nytimes.com/2022/12/22/video/russia-ukraine-bucha-massacre-takeaways.html.

nails. This grew public outrage and had a psychological impact as well. However, eventually it was learned that the Chinese army had more casualties than the Indian side. China also has a virtually closed internet model for the people, with exponential censorship. Which makes it harder for India or any other country to access information about the country.

### Lessons and Recommendations

Lessons for India are provided below in Strategic, Operational and Tactical levels respectively:

### Inculcate an intelligence culture and consider the role of Academia

A critical step in analysis is to first produce information to process intelligence. The role of Academia is crucial here to support the country's strategic intelligence. Opinions and assessments of experts in academia, who have worked on specific areas may provide insights and variables to perform a political-psychological analysis of national leaders. Academic research will help to monitor geopolitical events and identify key trends to keep up for India. Significant research should also be done on India's intelligence culture and provide critical insights to avoid the shortcomings Russia faced during the war.

### Monitor Foreign Science and Technology Intelligence

In addition to research, it is imperative to maintain continuous monitoring and surveillance of research conducted by foreign nations. Historical evidence demonstrates that periods of wars and conflicts have acted as catalysts for technological advancements. The Russia-Ukraine war, for instance, has seen the emergence of various novel technologies and warfare methods.[24] To remain vigilant and understand their potential implications for India, we must diligently monitor these developments using open sources.

The Chinese government virtually blocked the access of the international community to its open access journals.[25] The measure was triggered by a US based think tank, CSET on how the People's Liberation Army (PLA) has made significant progress adopting artificial intelligence for combat and support functions using US based company's semiconductor designs. Moreover, China's Science and technology monitoring has evolved considerably since 1958. The initiative has supported China's

[24[]] Ballinger, Ollie. 2022. "Radar Interference Tracker: A New Open Source Tool to Locate Active Military Radar Systems - bellingcat." Bellingcat. https://www.bellingcat.com/resources/2022/02/11/radar-interference-tracker-a-new-open-source-tool-to-locate-active-military-radar-systems/.; Palavenis, Donatas, and Vitaly Kuzmin. 2022. "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian W." Air Land Sea Space Application Center. https://www.alsa.mil/News/Article/3170285/the-use-of-emerging-disruptive-technologies-by-the-russian-armed-forces-in-the/.; Katz, Brian. 2020. "The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence." CSIS. https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence.

[25[]] Brar, Aadil, and Smruti Deshpande. 2023. "China is making national security a priority, starting with crackdown on open source data." ThePrint, April 17, 2023. https://theprint.in/opinion/china-is-making-national-security-a-priority-starting-with-crackdown-on-open-source-data/1522429/.

development of nuclear and other strategic weapons. While centrally directed, China's STI apparatus is distributed and functions at all levels in separate but interlocking organisations. Around 100,000 S&T intelligence workers consisting of open source collectors, analysts, and field operatives.[26]

Given the paramount importance of STI in shaping modern conflicts and technological advancements, India must stay informed about these developments. Being aware of the evolving landscape of scientific and technological advancements worldwide is essential for strategic preparedness and maintaining a competitive edge.

### Media literacy and national security awareness

The people of India will have to be informed about media literacy, and how to absorb information/news during domestic issues. After the 2014 Crimean invasion of Russia, Ukraine led an exponential information literacy for its people. This helped to counter disinformation at the individual level. The border population, both in the Eastern and Western Front have to be informed on the usage of social media and photography during troop movements in their neighbourhood. To avoid the adversaries OSINT desk to identify the details of military movements, must be created or strengthened.

### Access Commercial Off-the shelf Tools for Analysis

The commercial Off-the shelf tools used by companies to analyse their customer behaviour and shopping patterns, can be modified to military use for sentiment analysis. Political opinions of the domestic population should be taken into consideration when framing policies.

### Access and Control over Social Media

Most of the social media platforms used in India are US based companies. The government of India has obligated these companies to block accounts and remove posts flagged by them, however, we lack the sovereignty to access data of our population.[27] The Indian government's reach to their own people should not rely on a foreign based platform. The dynamic contemporary geopolitics may turn any friend to a foe and restrict access to information.

### Monitoring social media activities in geofenced areas during a crisis

The government of India's first standard measure during a domestic crisis is to block internet access. Entirely blocking the flow of information to counter disinformation could be inimical for collection of timely intelligence. Information retrieved from social media during domestic crises and conflicts does not only produce intelligence for situational awareness but also aid in providing digital evidence for violent crimes. Therefore, the

[26] Hannas, William, and Huey Chang. 2021. "China's STI Operations." Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/chinas-sti-operations/.

[27] The Hindu. 2021. "Govt announces new social media rules to curb its misuse." The Hindu, February 25, 2021. https://www.thehindu.com/news/national/govt-announces-new-social-media-rules/article33931290.ece.

government must  instead closely monitor the social media activities by geofencing areas of interest.

**Establish edge computing and OSINT desks at the Operational Level**

While New Delhi and other cities are equipped with supercomputers to process and analyse large data sets, it is important to establish edge computing and OSINT desks at the Operational level as well, to integrate all sources of intelligence and work closer with the end user.

**Less digital presence of the commander**

The digital data of a commander or a decision maker on the internet needs to be identified and evaluated. The application of Psychometrics, with variable inputs from publicly available data and intelligence from other sources can be used to predict the decisions of the commander. The Standard Operating Procedures (SOP) provided to the commanders during escalatory scenarios itself can be a foundational variable to the application. While we try to build defensive measures against these threats, we should attempt to do the same to our adversaries.

**Comprehensive Action plan to end all OSINT loopholes during a crisis**

Finally, India needs to develop a comprehensive Action Plan to end and control all OSINT loopholes during a crisis. The framing of the action plan should consider all levels, from national to the tactical level. At the national level, India could attempt to implement a closed or unplugged internet network in the country. Russia has also successfully tested the closed internet network system within the country.

## DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

## References

1. 109th Congress. (2005, May 20). SEC. 931. DEPARTMENT OF DEFENSE STRATEGY FOR OPEN-SOURCE INTELLIGENCE.
2. ABC News. (2022, March 2). A 64-kilometre-long Russian military convoy is approaching Kyiv. Here's what we know so far. *ABC*. Retrieved July 25, 2023, from https://www.abc.net.au/news/2022-03-02/a-massive-russian-convoy-is-approaching-kyiv-heres-what-we-know/100874820
3. Abdalla, N. S., Davies, P. H., Gustafson, K., Lomas, D., & Wagner, S. (2022, May 11). *Intelligence and the War in Ukraine: Part 1.* Retrieved July 21, 2023, from War on the Rocks: https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-2/

4. Abdalla, N. S., Davies, P. H., Gustafson, K., Lomas, D., & Wagner, S. (2022, May 11). *Intelligence and the War in Ukraine: Part 1.* Retrieved July 21, 2023, from War on the Rocks: https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/
5. Amos, D. (2022, June 12). Open source intelligence methods are being used to investigate war crimes in Ukraine. *NPR*. Retrieved July 24, 2023, from https://www.npr.org/2022/06/12/1104460678/open-source-intelligence-methods-are-being-used-to-investigate-war-crimes-in-ukr
6. Andre, D. (2017, December 12). *Seeing the Forest Through the Trees: The Value of OSINT for the U.S. Navy | Center for International Maritime Security.* Retrieved July 25, 2023, from Cimsec: https://cimsec.org/seeing-forest-trees-value-osint-u-s-navy/
7. Ballinger, O. (2022, February 11). *Radar Interference Tracker: A New Open Source Tool to Locate Active Military Radar Systems - bellingcat.* Retrieved July 20, 2023, from Bellingcat: https://www.bellingcat.com/resources/2022/02/11/radar-interference-tracker-a-new-open-source-tool-to-locate-active-military-radar-systems/
8. BBC News. (2022, April 11). Ukraine conflict: Why is Russia losing so many tanks? *BBC*. Retrieved July 25, 2023, from https://www.bbc.com/news/world-61021388
9. Bellingcat. (n.d.). *Bellingcat Radar Interference Tracker.* Retrieved July 26, 2023, from Earth Engine Apps: https://ollielballinger.users.earthengine.app/view/bellingcat-radar-interference-tracker#lon=49.9507;lat=26.6056;zoom=4;
10. Benjamin, A. (2023, January 16). *The importance of OSINT in the air war in Ukraine.* Retrieved July 18, 2023, from OSINT for Ukraine: https://www.osintforukraine.com/publications/the-importance-of-osint-in-the-air-war-in-ukraine
11. Bergengruen, V. (2022, April 18). *How Ukraine Is Crowdsourcing Digital Evidence of War Crimes.* Retrieved July 23, 2023, from Time: https://time.com/6166781/ukraine-crowdsourcing-war-crimes/
12. Brar, A., & Deshpande, S. (2023, April 17). China is making national security a priority, starting with crackdown on open source data. *ThePrint*. Retrieved July 25, 2023, from https://theprint.in/opinion/china-is-making-national-security-a-priority-starting-with-crackdown-on-open-source-data/1522429/
13. Brown, Z. T., & Medina, C. A. (2021, March 9). *The Declining Market for Secrets.* Retrieved July 18, 2023, from Foreign Affairs: https://www.foreignaffairs.com/united-states/declining-market-secrets
14. Browne, M. (2022, December 22). Caught on Camera, Traced by Phone: The Russian Military Unit That Killed Dozens in Bucha. *The New York Times*. Retrieved July 23, 2023, from https://www.nytimes.com/2022/12/22/video/russia-ukraine-bucha-massacre-takeaways.html
15. Carrée, L. (2023, February 2). *The Role Of Technology In The Exposition Of War Crimes In Ukraine: How The Use Of Cutting-Edge Technologies And Open-Sources Investigations Can Expose Human Rights Violations.* Retrieved July 21, 2023, from LSE Blogs: https://blogs.lse.ac.uk/humanrights/2023/02/02/the-role-of-technology-in-the-exposition-of-war-crimes-in-ukraine-how-the-use-of-cutting-edge-technologies-and-open-sources-investigations-can-expose-human-rights-violations/
16. China Tech Team. (2023, April 18). *The Challenges of Conducting Open Source Research on China - bellingcat.* Retrieved July 27, 2023, from Bellingcat: https://www.bellingcat.com/resources/2023/04/18/china-challenges-open-source-osint-social-media/
17. Cranny, S. (2022, March 9). *Russian Comms in Ukraine: A World of Hertz.* Retrieved July 22, 2023, from RUSI: https://rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz

18. Davies, P. H. (2022, May 20). *No War for Old Spies: Putin, the Kremlin and Intelligence.* Retrieved July 25, 2023, from RUSI: https://rusi.org/explore-our-research/publications/commentary/no-war-old-spies-putin-kremlin-and-intelligence
19. Dylan, H., Gioe, D. V., & Grossfield, E. (n.d.). The autocrat's intelligence paradox: Vladimir Putin's (mis)management of Russian strategic assessment in the Ukraine War. *The British Journal of Politics and International Relations, 25*(3).
20. E, P. (2018, December 13). *The Tactical Application of Open Source Intelligence (OSINT) | The Cove.* Retrieved July 15, 2023, from The Cove: https://cove.army.gov.au/article/tactical-application-open-source-intelligence-osint
21. Ford, M., & Hoskins, A. (2022). *Radical War: Data, Attention and Control in the Twenty-First Century.* Oxford University Press. Retrieved July 23, 2023
22. Gill, R. (2023, February 23). *What is OSINT (Open-Source Intelligence?).* Retrieved July 17, 2023, from SANS Institute: https://www.sans.org/blog/what-is-open-source-intelligence/
23. Gordon, J. D. (2019, January 14). *Operationalizing OSINT Full-Spectrum Military Operations.* Retrieved July 20, 2023, from Small Wars Journal: https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations
24. Hannas, W., & Chang, H. (2021, January). *China's STI Operations.* Retrieved July 25, 2023, from Center for Security and Emerging Technology: https://cset.georgetown.edu/publication/chinas-sti-operations/
25. Harding, L. (2021, February 21). Eliot Higgins: 'People accuse me of working for the CIA'. *The Guardian*. Retrieved July 26, 2023, from https://www.theguardian.com/media/2021/feb/20/eliot-higgins-people-accuse-me-of-working-for-the-cia
26. Harrington, J., & McCabe, R. (2021, August 6). *Modernizing Intelligence, Surveillance, and Reconnaissance to 'Find' in the Era of Security Competition.* Retrieved July 18, 2023, from CSIS: https://www.csis.org/analysis/modernizing-intelligence-surveillance-and-reconnaissance-find-era-security-competition
27. Harvey, A. S. (2021, November-December). The Levels of War as Levels of Analysis. *Military Review*, 75-81.
28. Harwell, D., & Polk, G. (2022, April 15). Ukraine using ClearviewAI facial recognition to identify Russian war dead. *Washington Post*. Retrieved July 18, 2023, from https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/
29. Hewson, J. (2023, March 2). *A Private Company Is Using Social Media to Track Down Russian Soldiers.* Retrieved July 19, 2023, from Foreign Policy: https://foreignpolicy.com/2023/03/02/ukraine-russia-war-military-social-media-osint-open-source-intelligence/
30. Horbyk, R. (2022, October 21). "The war phone": mobile communication on the frontline in Eastern Ukraine. *Digital War, 3*, 9-24.
31. How open-source intelligence has shaped the Russia-Ukraine war. (2022, December 09). GOV.UK.
32. Ismay, J. (2022, March 30). Putin's Advisers Misinformed Him on Ukraine, U.S. Intelligence Suggests. *The New York Times*. Retrieved July 25, 2023, from https://www.nytimes.com/2022/03/30/world/europe/putin-advisers-ukraine.html
33. Janjeva, A., Harris, A., & Byrne, J. (2022, June). The Future of Open Source Intelligence for UK National Security. Royal United Services Institute.

34. Jones, S. G. (2022, June 1). *Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare.* Retrieved July 25, 2023, from CSIS: https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare
35. Karalis, M. (2022, December 16). *Open-source intelligence in Ukraine: Asset or liability?* Retrieved July 18, 2023, from Chatham House: https://www.chathamhouse.org/2022/12/open-source-intelligence-ukraine-asset-or-liability
36. Karalis, M. (2022, December 16). *Open-source intelligence in Ukraine: Asset or liability?* Retrieved July 20, 2023, from Chatham House: https://www.chathamhouse.org/2022/12/open-source-intelligence-ukraine-asset-or-liability
37. Katz, B. (2020, April 17). *The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence.* Retrieved July 24, 2023, from CSIS: https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence
38. Kofman, M., & Michaels, J. (2022, May 18). *Ukraine: The Daily Intelligence Event | Royal United Services Institute.* Retrieved July 21, 2023, from RUSI: https://rusi.org/explore-our-research/publications/commentary/ukraine-daily-intelligence-event
39. Lindley, J. (2023, June 27). *The Russo-Ukraine-Western Intelligence War – Aspenia Online.* Retrieved July 23, 2023, from Aspenia Online: https://aspeniaonline.it/the-russo-ukraine-western-intelligence-war/
40. Lindley, J. (2023, June 27). *The Russo-Ukraine-Western Intelligence War – Aspenia Online.* Retrieved July 25, 2023, from Aspenia Online: https://aspeniaonline.it/the-russo-ukraine-western-intelligence-war/
41. Lomas, D. (2023, July 5). *The Death of Secret Intelligence? Think Again | Royal United Services Institute.* Retrieved July 21, 2023, from RUSI: https://rusi.org/explore-our-research/publications/commentary/death-secret-intelligence-think-again
42. Mackinnon, A. (2020, December 17). *How Bellingcat's Open Source Investigations Help the Work of U.S. Intelligence Agencies.* Retrieved July 21, 2023, from Foreign Policy: https://foreignpolicy.com/2020/12/17/bellingcat-can-say-what-u-s-intelligence-cant/
43. Mercado, S. (2004). Sailing the Sea of OSINT in the Information Age. *Studies in Intelligence, 48*(3), 45-55.
44. Miller, G., & Medvedchuk, V. (2022, August 19). FSB errors played crucial role in Russia's failed war plans in Ukraine. *Washington Post*. Retrieved July 23, 2023, from https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/
45. Mitzer, S. (2022, February 24). *Attack On Europe: Documenting Russian Equipment Losses During The Russian Invasion Of Ukraine.* Retrieved July 25, 2023, from Oryx: https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html
46. Palavenis, D., & Kuzmin, V. (2022, October 1). *The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian W.* Retrieved July 25, 2023, from Air Land Sea Space Application Center: https://www.alsa.mil/News/Article/3170285/the-use-of-emerging-disruptive-technologies-by-the-russian-armed-forces-in-the/
47. Panella, C. (2023, June 24). Putin's Presidential Plane Spotted Leaving Moscow Amid Wagner Uprising. *Business Insider*. Retrieved July 25, 2023, from https://www.businessinsider.in/international/news/putins-presidential-plane-was-spotted-leaving-moscow-amid-wagners-uprising/articleshow/101245115.cms

48. Rasak, C. J. (2021, January). Event Barraging and the Death of Tactical Level Open-Source Intelligence. *Military Review*, 48-57.
49. Reuter, M., Dobusch, L., & Först, V. (2022, March 2). *OSINT in the Ukraine: Putting the Pieces in Place – netzpolitik.org.* Retrieved July 22, 2023, from Netzpolitik: https://netzpolitik.org/2022/osint-in-the-ukraine-putting-the-pieces-in-place/
50. Rovner, J. (2022, May 23). *Intelligence and War: Does Secrecy Still Matter?* Retrieved July 21, 2023, from War on the Rocks: https://warontherocks.com/2022/05/intelligence-and-war-does-secrecy-still-matter/
51. Salerno-Garthwaite, A. (n.d.). *OSINT in Ukraine: civilians in the kill chain and the information space.* Retrieved July 23, 2023, from Global Defence Technology: https://defence.nridigital.com/global_defence_technology_oct22/osint_in_ukraine
52. Sutton, H. (2022, February 15). *Covert Shores.* Retrieved July 20, 2023, from H I Sutton - Covert Shores: http://www.hisutton.com/Russia-Med-BS-2022-02-15.html
53. Taddeo, M., Floridi, L., & Ghioni, R. (2023, February 17). *Open Source Intelligence (OSINT) and AI: The Informational Pivot of Intelligence Analysis.* Retrieved July 21, 2023, from Oxford Internet Institute: https://www.oii.ox.ac.uk/news-events/news/open-source-intelligence-osint-and-ai-the-informational-pivot-of-intelligence-analysis/
54. Team Mighty. (2023, March 16). *Russian soldiers in Ukraine are being hunted using social media.* Retrieved July 26, 2023, from We Are The Mighty: https://www.wearethemighty.com/articles/russian-soldiers-in-ukraine-are-being-hunted-using-social-media/
55. The Economist. (2021, August 7). The promise of open-source intelligence. *The Economist*. Retrieved July 21, 2023, from https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence
56. The Hindu. (2021, February 25). Govt announces new social media rules to curb its misuse. *The Hindu*. Retrieved July 25, 2023, from https://www.thehindu.com/news/national/govt-announces-new-social-media-rules/article33931290.ece
57. *track aircraft live.* (n.d.). Retrieved July 20, 2023, from track aircraft live: https://globe.adsbexchange.com/
58. TZ, & Hayman, T. (2023, January 5). *Open-Source Intelligence and the War in Ukraine.* Retrieved July 21, 2023, from INSS: https://www.inss.org.il/publication/russia-ukraine-intelligence/
59. *Ukrainians are changing approaches to modern warfare. Here is how.* (2023, January 31). Retrieved July 26, 2023, from Russia's war in Ukraine: https://war.ukraine.ua/articles/ukrainian-innovations-are-changing-approaches-to-modern-warfare/
60. United Nations for Human Rights Office of the High Commissioner. (2022). *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law.* UN. Retrieved July 26, 2023
61. Vandersmith, M. (2023, March). How Open-Source Intelligence Is Changing Warfare. *The Naval Review, 149*(3), 1441.
62. Vasilyev, P. (2023, June 6). Nova Kakhovka Hydroelectric Station destroyed. What we know about the breach and interpretations from Ukraine, Russia, and OSINT researchers. *Mediazona*. Retrieved July 24, 2023, from https://en.zona.media/article/2023/06/06/kakhovka

63. Vinci, A. (2020, August 31). *The Coming Revolution in Intelligence Affairs.* Retrieved July 18, 2023, from Foreign Affairs: https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs
64. Wakefield, J. (2019, December 24). *Russia 'successfully tests' its unplugged internet.* Retrieved July 20, 2023, from BBC: https://www.bbc.com/news/technology-50902496
65. Waller, J. (2023, June 14). *Intelligence Failures and Political Misjudgment in an Age of Ideological Change.* Retrieved July 27, 2023, from The Strategy Bridge: https://thestrategybridge.org/the-bridge/2023/6/14/intelligence-failures-and-political-misjudgment-in-an-age-of-ideological-change
66. Walton, C. (2023, July 19). *The New Spy Wars: How China and Russia Use Intelligence Agencies to Undermine America.* Retrieved July 16, 2023, from Foreign Affairs: https://www.foreignaffairs.com/china/russia-china-intelligence-new-spy-wars-undermine-america
67. Weinbaum, C. (2018). *Perspectives and Opportunities in Intelligence for U.S. Leaders.* RAND Corporation. Retrieved July 18, 2023
68. Weinbaum, C., Berner, S., & McClintock, B. (2017). *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain | RAND.* Retrieved July 20, 2023, from RAND Corporation: https://www.rand.org/pubs/perspectives/PE273.html
69. Weinbaum, C., Parachini, J. V., & Williams, J. (2021, April 12). *The Intelligence Community's Deadly Bias Toward Classified Sources.* Retrieved July 16, 2023, from RAND Corporation: https://www.rand.org/blog/2021/04/the-intelligence-communitys-deadly-bias-toward-classified.html
70. Williams, H. J., & Blum, I. (2018). *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* RAND Corporation. Retrieved July 26, 2023
71. Winter, C., Gallacher, J., & Harris, A. (2023, February 21). *Artificial Intelligence, OSINT and Russia's Information Landscape | Centre for Emerging Technology and Security.* Retrieved July 20, 2023, from Centre for Emerging Technology and Security: https://cetas.turing.ac.uk/publications/artificial-intelligence-osint-and-russias-information-landscape
72. Ziółkowska, A. (2018, February). Open source intelligence (OSINT) as an element of military recon. *Security and Defence Quaterly, 19*(2), 65-77.