Informatyka techniczna i sztuczna inteligencja
Technical informatics and Artificial Intelligence
Engineer of XXI Century'2024

OSINT in the context of war as an example of russia's invasion in Ukraine

Tetiana Savkova [1], Oleh Harasymchuk [2,*], Yaroslav Sovyn [3]

[1] *Lviv Polytechnic National University, 12 Bandera St., Lviv 79013, Ukraine, tetiana.savkova.kb.2021@lpnu.ua*
[2] *Lviv Polytechnic National University, 12 Bandera St., Lviv 79013, Ukraine, oleh.harasymchuk@gmail.com*
[3] *Lviv Polytechnic National University, 12 Bandera St., Lviv 79013, Ukraine, sovynjarosl@gmail.com*
* *Corresponding author, oleh.harasymchuk@gmail.com*

Abstract: The main purpose of this study is to analyze the role of OSINT in hybrid warfare with a specific focus on the Russian-Ukrainian war. The research examines key innovations, figures, organizations, and tools relevant to OSINT, aiming to identify technological challenges and ethical considerations. Additionally, this study seeks to propose practical approaches for optimizing OSINT practices and highlight their strategic advantages in modern wars. To find out the opportunities, challenges, and limitations of using OSINT in military operations and to reveal ways to overcome them.

Keywords: OSINT, russian-ukrainian war, open source intelligence, war crimes, military intelligence, geospatial data, propaganda, social media, satellite imagery, cyber hygiene, key figures;

OSINT w kontekście wojny na przykładzie inwazji rosji na Ukrainę

Tetiana Savkova [1], Oleh Harasymchuk [2,*], Yaroslav Sovyn [3]

[1] *Uniwersytet Narodowy Politechnika Lwowska, ul. St. Bandery 12, Lwów 79013, Ukraina, tetiana.savkova.kb.2021@lpnu.ua*
[2] *Uniwersytet Narodowy Politechnika Lwowska, ul. St. Bandery 12, Lwów 79013, Ukraina, oleh.harasymchuk@gmail.com*
[3] *Uniwersytet Narodowy Politechnika Lwowska, ul. St. Bandery 12, Lwów 79013, Ukraina, sovynjarosl@gmail.com*

* *Corresponding author, oleh.harasymchuk@gmail.com*

Streszczenie: Głównym celem rozwiązania tego badania jest rozważenie nowoczesnych metod i technologii wywiadowczych opartych na otwartych źródłach, OSINT i ich roli w kontekście wojny rosyjsko-ukraińskiej. Badania mają na celu analizę skuteczności wykorzystania OSINT w wykrywaniu zbrodni wojennych, analizę ruchu wojsk i sprzętu, a także wykrywanie materiałów propagandowych i określenie możliwości jego wykorzystania w celu przeciwdziałania agresywnej polityce. Aby dowiedzieć się o szansach, wyzwaniach i ograniczeniach wykorzystania OSINT w operacjach wojskowych i ujawnić sposoby ich przezwyciężenia.

Słowa kluczowe: OSINT, wojna rosyjsko-ukraińska, wywiad typu open source, zbrodnie wojenne, wywiad wojskowy, dane geoprzestrzenne, propaganda, media społecznościowe, zdjęcia satelitarne, cyberhigiena, kluczowe postacie;

1. Introduction

In the era of hybrid warfare, where information operations play a critical role alongside physical combat, Open-Source Intelligence, also known as OSINT, has emerged as an essential tool. Its role becomes even more pronounced in the context of the russian-Ukrainian war, in which russia is the undisputed aggressor, cybersecurity is almost one of the main frontiers in the fight for justice in the digital space.

DOI: https://doi.org/10.53052/9788367652292.27

A thorough examination of images and videos, whether of traces of rocket fire or evidence of executions, is key in the investigation of war crimes. Basic tools such as satellites, unmanned aerial vehicles, various software, and intelligence based on open sources play an equally important role. Therefore, in this publication based on strong information sources, we recognize how OSINT can become a reliable source for reviewing these crimes and even more - their countermeasures.

Several key aspects can be identified by analyzing publicly available data, using social media, news, and geospatial data and re-analyzing recent research and publications on the use of OSINT in the context of the russian-Ukrainian war. Research focuses on the methods and technologies used to collect and analyze information from various sources.

In addition, based on research, in hybrid war it is possible to apply the effectiveness and importance of using OSINT in detecting propaganda materials, analyzing the movement of military and equipment, as well as detecting war crimes of the aggressor country. Some of them also pay attention to the ethical and legal aspects of the use of OSINT in military activities, including issues of confidentiality, data reliability, and the legitimacy of the use of information sources. Nevertheless, the question arises as to how the conclusions based on the open-source investigation can be made legally sound in future proceedings. This analysis reflects the growing interest in using OSINT in military conflicts (in our case, wars) and identifies the advantages and challenges associated with such an approach [1].

The main purpose and objective of this study is to examine the role of open-source intelligence, OSINT, in the context of the Russian-Ukrainian war. The study aims to analyze the effectiveness of OSINT in detecting war crimes, analyzing the movement of troops and equipment, as well as identifying propaganda materials and determining the possibilities of using it to counteract aggressive policies. To identify possible challenges and limitations of using OSINT in military operations and to reveal ways to overcome them.

2. OSINT

2.1. OSINT Basics

Open-Source Intelligence or OSINT is the intelligence based on open sources, that is, with open-source code. All information is gathered through public sources and then processed, synthesized, and analyzed into intelligence.

The above definition of the concept of OSINT is quite generalized since today no phrase can fully describe this type of intelligence, covering all its aspects. However, there is a kind of NATO manual - "NATO Open-Source Intelligence Handbook" (can include scientific reports, technical instructions, economic reports, working documents, non-official government documents, dissertations, marketing studies, newsletters, and much more [2]. All materials cover a scientific purpose, political, socio-economic, and military sphere). And it is in it that you are most likely to find not only the most accurate definition but also the basic instructions for the development of OSINT, using accompanying documents such as: "Intelligence Exploitation of the Internet" and "NATO OSINT Reader" - commanders and their staffs have basic instructions on the development of OSINT [3-4].

In general, OSINT relies on a wide range of information and sources, including:

- Mass media: newspapers, magazines, radio, television, and other computer information.
- Public data: Information obtained from government reports; official data, such as data on budgets and demographic indicators; hearing; legislative debates; press conferences, speeches, handbooks, organizational charts, maritime and aviation safety warnings, environmental impact statements, contracts and required financial disclosures, and other public sources.
- The proliferation of worldwide satellite imagery, often in high resolution, on the Internet (such as Google Earth) is expanding the public's ability to obtain information previously only available to mainstream intelligence.

The peculiarity is that this intelligence method is legal, the necessary information with which the OSINT specialist works and which is listed above is open, and there are no other illegal actions.

However, everything is not so simple, because every specialist is faced with huge amounts of data that appear on the Internet almost every second [9]. That is why analyzing everything and finding the main thing among the endless stream of available data is quite a difficult process. So this is one of the challenges the open source intelligence community is facing. Moreover, the information that will ultimately be considered "the same" is subject to detailed verification, because it may be deliberately distorted, inaccurate, or banally outdated. Therefore, the key task at this stage is to see what is a fact and what is not, and based on this to reproduce a realistic model of events[6].

Based on this, it is possible to form a table of sequences (see Figure 1) [8]:

Although this type of intelligence is legal, there is a fine line in obtaining and using data that is quite easy to cross.

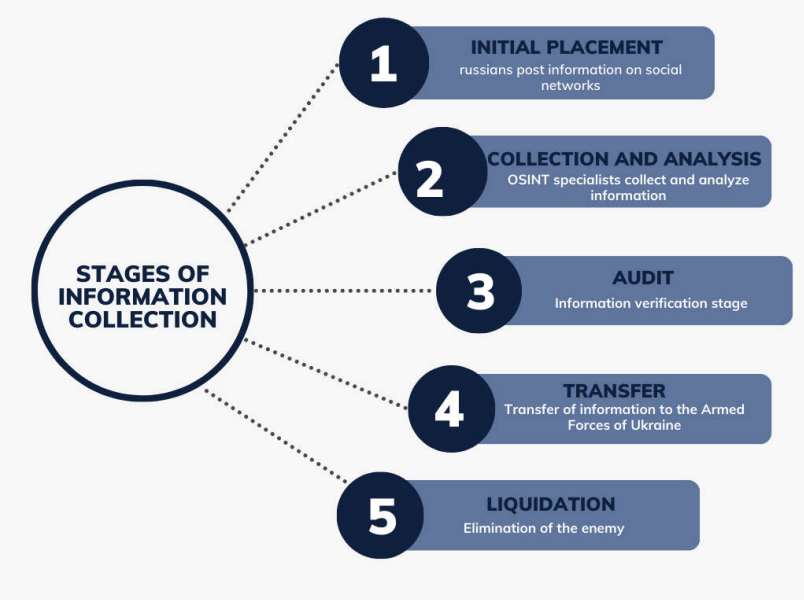

Figure 1. Stages of information collection

Currently, there are many tools that OSINT analysts use in their work. From global search tools to people search tools or web scrapers. You can read more about them in the book "Open-Source Intelligence Tools and Resources Handbook 2020" [5].

Not to be missed is the discussion on the history of the Foreign Broadcasting and Open-Source Intelligence Service that was presented by Admiral William Studeman at the First International Symposium on Open Source Solutions in December 1992.

Admiral William said the following words:

"In some cases, intelligence analysts believe that information from open sources is more accurate than classified sources. This may derive either from the weight and credibility of open sources compared to the unverified, controversial, or poor nature of classified sources, or from some other evaluative criteria. When we prefer unclassified sources to classified sources, we must be sensitive to the credence we place on the data, taking it as our position.

Most people in our business agree that open source has proven extremely valuable for intelligence. Even during the Cold War, when intelligence was focused mainly on obtaining classified information, open sources gave us very useful glimpses into closed societies.[7] "

These words were spoken in 1992, but they have not lost their relevance even today.

The availability and usefulness of OSINT depend and will depend on the specific area of operations under consideration, as well as two other factors: the level of hostilities and the point on the spectrum of conflict, from presence to general war, where the intelligence will be applied. Overall, OSINT has significant potential as a source of intelligence support for detection, prevention, policy development, contingency planning, security, assistance, arms acquisition (development and countermeasures), and tactical operations against emerging priorities such as the proliferation of weapons of mass destruction. damage OSINT is vital as a means of quickly orienting the commander and serves as the basis for intelligence collection and management.

2.2. OSINT and the Military

Viewed at the ***strategic level***, OSINT can provide certain indications and warnings of both enemy intent and opportunities for military advantage. Content analysis of multiple open sources, such as regional newspapers, is often, if not always, a more reliable basis for assessing stability and instability than reports from secret sources with limited access and personal views that bias information (Recall the aforementioned speech by Admiral William).

Of particular value is the cultural and demographic intelligence that OSINT conducts in areas not typically well covered by traditional civilian and military intelligence gathering and analysis. In addition, OSINT can provide very important geographic and civil generalizations that can significantly influence major military acquisitions can significantly influence important military procurement and design decisions. OSINT can provide unclassified threat intelligence that can be used to train and mobilize public and political support for military needs, including policy development.

Viewed at the ***operational level***, OSINT can provide the geographic and civil intelligence necessary for regional military planning and deployment of armed forces. In particular, OSINT has developed a reliable regional overview of the air, ground, and naval capabilities that the tactical group commander may face; geographic generalizations regarding cross-country mobility, average line-of-sight distances, temperatures, and water availability; and civilian generalizations such as loading bridges, clearing ports, bunkering aircraft; civilian communication and computing resources. OSINT provides prompt solutions to the theater commander's questions about civilian infrastructure, political cliques and personalities, and economic and financial factors affecting the operational deployment of troops, and is therefore particularly useful for unsupported contingency planning from traditional means of intelligence.
OSINT is particularly useful to the theater commander for coordinating joint and coalition operations where traditional classified intelligence tools are either unavailable or cannot be provided to foreign elements.
At the ***tactical level***, OSINT has proven its relevance and effectiveness in countering the proliferation of weapons of mass destruction, combating terrorism, and assisting peacekeeping operations. This applies both to conventional military operations aimed at overt interception and to covert or covert "direct action" operations by special operations forces.
OSINT is a critical resource for a military command that requires maps and digital information to target targets.
Looking at it at a ***technical level***, OSINT intelligence on civilian communications and computer capabilities in the area of operations will be deployed for the team. As information warfare becomes a critical enabler and all adversaries achieve certain elements of electronic warfare, the commander must use OSINT both to understand how to reduce the effectiveness of civilian forces and assets employed by the adversary and to identify opportunities for the use of civilian means to support joint and coalition communications.
Based on this, you can form a table of OSINT levels (see Figure 2):

Figure 2. OSINT levels

Returning to the realities of the russian-Ukrainian war, we can well project the above general levels of OSINT to the current situation.
Military-wise, OSINT has allowed the Ukrainian military to track the movements, plans, and operations of russian forces. Satellite images gave Ukrainians information about the areas attacked by russian troops. Unencrypted radio waves and mobile phones allowed Ukrainians to eavesdrop on russian communications. Social media posts from both russian soldiers and Ukrainian citizens showed what the war looks like on the ground, providing Ukrainian officials with information about where and how russian forces are operating. These advantages provided by OSINT allowed Ukraine to resist russian aggression.

2.3. Key Innovations in OSINT Automation

We believe that the automation of OSINT in the russian-Ukrainian war has been pivotal in enhancing the speed and accuracy of intelligence gathering. The integration of machine learning, AI, and automated pipelines has significantly improved the real-time processing of vast amounts of publicly available data. This not only aids in strategic decision-making but also enables quicker and more efficient responses, compared to traditional intelligence methods.

It is worth to mention the main **key innovations in OSINT automation**:

1. Real-Time Event Detection and Analysis

Tools like ExTrac utilize AI to track events and detect patterns within large datasets, including social media and news sources. For instance, ExTrac was crucial in identifying key events around Bucha and Kyiv, enabling Ukraine to assess russian media narratives in real-time. The ability to track events immediately is critical for quick response and decision-making in a rapidly changing cwar environment.

2. Social Media Scraping and Verification

Automation tools such as Hunchly are used to monitor social media for signs of disinformation or to locate russian military units. Data extracted from these platforms is analyzed using tools like Google Earth Pro and GeolocOSINT, which can verify the geolocation of photos and videos. This process is crucial for confirming the authenticity of public content, especially in real-time, as citizens upload footage that can either provide evidence or spread disinformation.

3. Crowdsourced Intelligence and Automated Data Filtering

Platforms like MapHub have been essential for crowdsourced intelligence, where citizens upload geotagged photos or videos. Automated tools like ExifTool are employed to verify the authenticity of these submissions. This combined approach of crowdsourcing and automated filtering has helped Ukrainian forces target russian convoys with precision by validating real-time intelligence from the ground.

4. AI-Powered Video and Image Analysis

AI-driven tools like InVID and PimEyes analyze video content to verify authenticity, identify faces, and detect military equipment in the context of the war. This is crucial for tracking individuals within russian military units or verifying claims related to war crimes. These AI tools use advanced image recognition algorithms to match visual content against existing databases or patterns of military activity.

5. Automated OSINT Pipelines

Custom scripts in Python or R automate key tasks such as data scraping, keyword monitoring, and report generation. These automated workflows streamline the process of compiling intelligence from diverse sources, including social media, forums, and news outlets. By focusing on automated data collection, Ukraine's OSINT teams can devote more time to analyzing results and less to manual information gathering war.

6. Machine Learning for Predictive Analytics

Machine learning tools analyze war-related data patterns to predict possible outcomes, including troop movements and escalation points. These predictive models help Ukrainian forces anticipate changes in russian military tactics, allowing for a more agile response. The ability to forecast future developments can provide a strategic edge in an ongoing war(see Figure 3).

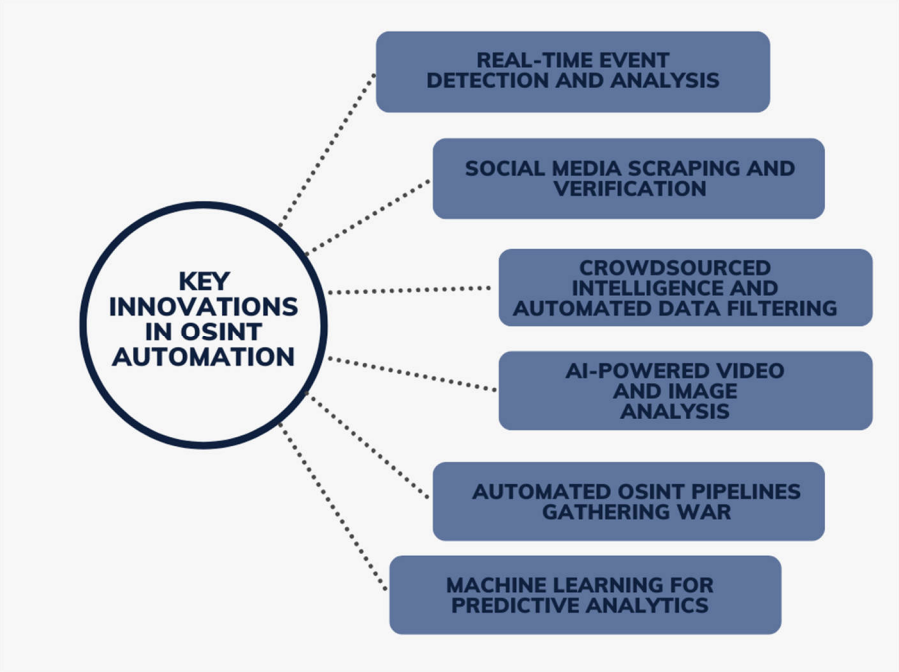

Figure 3. Key innovations in OSINT automation

Let us examine some real examples of OSINT automation in action. The first one is tracking russian disinformation. OSINT automation played a critical role in tracing and debunking the shifting narratives of russian disinformation, such as false flag operations. These automated systems were able to track changes in the information landscape in real-time, allowing analysts to rapidly counter misleading reports and prevent the spread of false information.

The second one is satellite imagery analysis. AI-powered tools like those from Maxar Technologies have been instrumental in analyzing satellite imagery to detect military activity. These AI models classify objects within satellite images to track russian troop movements and infrastructure destruction. This automation not only speeds up the analysis process but also enables continuous monitoring of large geographical areas, something that would be nearly impossible manually.

In comparison to traditional intelligence methods, these innovations streamline OSINT processes and provide Ukraine with a faster, more accurate means of countering russian aggression. By automating critical tasks, Ukraine can enhance military operations, improve strategic decisions, and remain ahead in the information warfare battle. These developments highlight the transformative impact of AI and machine learning in modern wars.

Ultimately, the integration of AI into OSINT represents a leap forward in war analysis, with wide-reaching implications for the future of military intelligence. The automation of OSINT not only ensures more timely intelligence but also enhances the effectiveness of countermeasures against misinformation and military movements [23].

2.4. Key Figures in OSINT Investigations

Worth to mention that the Operational Taskforce (OTF) created by Europol to assist in ongoing investigations of major international crimes committed in Ukraine following the invasion of russian armed forces in February 2022.

The OTF helps identify suspects and their involvement in war crimes, crimes against humanity, or crimes of genocide committed in Ukraine through the collection and analysis of open-source intelligence (OSINT) [10, 22].

The work of journalists, in particular those who work at Bellingcat [18], cannot be overlooked either. It is an investigative journalism group created by Elliot Higgins. Originally using the pseudonym Brown Moses, Higgins tracked and deleted information from hundreds of YouTube channels, Twitter feeds [21], and WhatsApp groups, looking for images and footage of weapons used in the Syrian civil war and by whom. Many of his reports were picked up by the media and human rights groups, exposing the horrific stories of the war. For example, Higgins compiled a database of 491 videos of cluster bombs being used across Syria, along with links to maps and details of the type of weapon used [11].

After Higgins' initial investigations in Syria, the British OSINT researcher recruited a team of experts, turning Bellingcat into one of the world's leading investigative journalism organizations.

Bellingcat identified those involved in the crash of the Malaysian Boeing 777 in the skies over Donbas in 2014. They proved that the Buk air defense system, which shot down the plane, belonged to the 53rd anti-aircraft missile brigade of the russian air force. The missile was transported to the occupied part of Donbas to be launched from Ukrainian territories, but immediately after the operation was returned to the aggressor country [19]. This is just one of the stories uncovered by this research group. We can also mention the disclosure of the activities of the terrorist Islamic State in Syria, in particular, the determination of the location of one of the "tops" of the ISIS terrorist group using only photos on social media. networks and using Google Maps. Bellingcat is also known for its work on determining the positions of sarin rockets during the bombing of Damascus on August 21, 2013. There are many such examples, but not all of them are known [12, 17].

Bellingcat is also at the forefront of OSINT in Ukraine. One of their investigations revealed the use of cluster munitions—weapons specifically designed to cause civilian casualties—against non-military targets in Ukraine (see Figure 4).

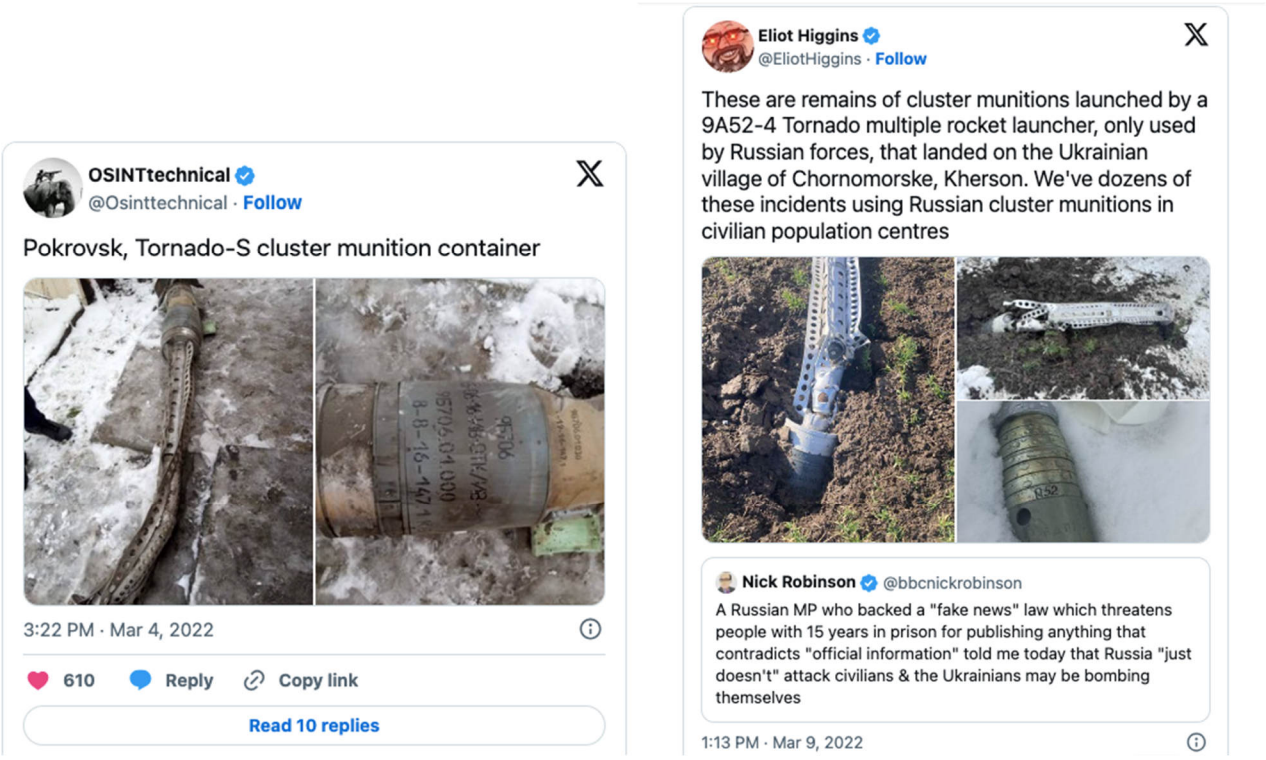

Figure 4. Bellingcat investigation into the use of cluster munitions by russian forces

Other Twitter accounts, such as Caliber Obscura and Oryx, documented footage of the war posted online and kept tallies of the various heavy casualties on both sides (see Figure 5).

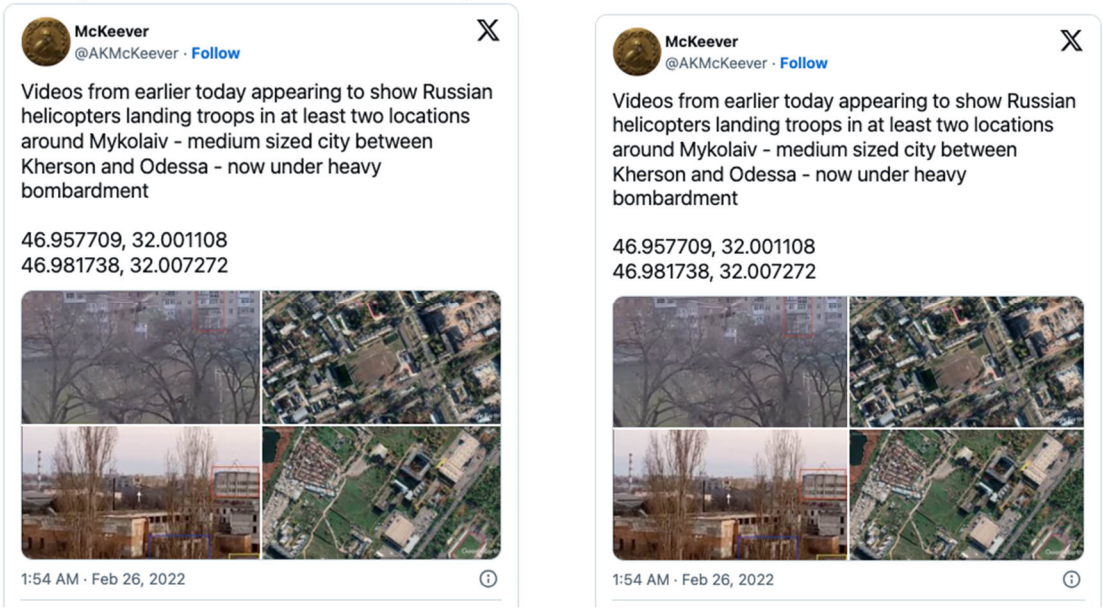

Figure 5. Footage of the war in Ukraine from the Caliber Obscura and Oryx investigation

It is worth saying that before the full-scale invasion, OSINT groups focused more on corrupt activities, but since the russian attack on Ukraine, OSINT investigative groups began to be actively formed in the country in the field of data analysis, specifically related to the military sphere and everything that affects the course of the war as such, covering a much wider field of activity.

Such groups became InformNapalm [13], the center of "Peacemaker" [16]. InformNapalm analyzes the data of local residents of Donbas and russian military personnel using their social media accounts. networks Thus, they determined the location of several military units of the russian Federation in the East, as well as the fact that tanks were regrouped

on the territory of Ukraine from the russian side, etc. [14-15]. And "Mirotvorets", in turn, publishes personal data of members of illegal armed formations of the russian Federation.

Space technology company Maxar, which provides real-time satellite imagery, also played a significant role at the time, publishing images of the ominous "40-mile russian convoy" advancing on Kyiv. Below is part of a russian military convoy near Ivankovo, Ukraine, February 28, 2022 (see Figure 6).

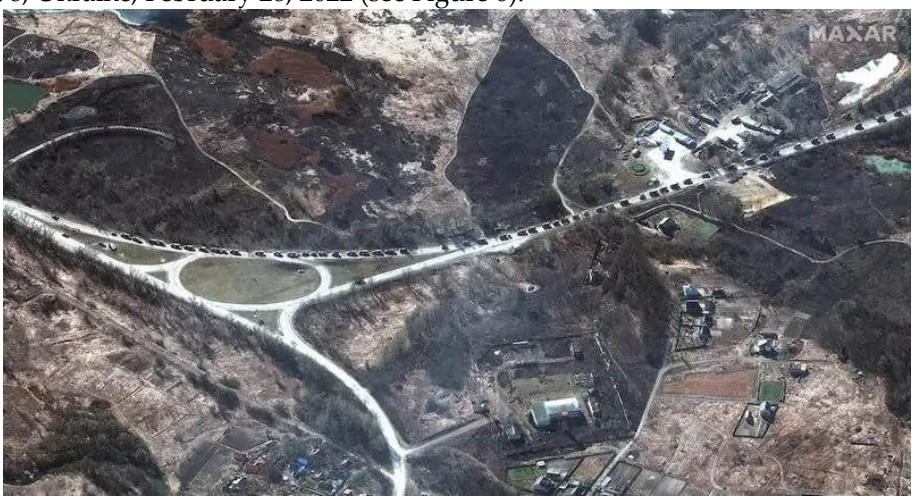

Figure 6. russian military convoy near Ivankovo, Ukraine, February 28, 2022 (Source: Maxar Technologies)

On February 24, 2022 (a few hours before the russian invasion), arms control expert Jeffrey Lewis, who heads a group of analysts at the Middlebury Institute of International Studies in Vermont, published a traffic jam on Google Maps that had formed on a road near the Ukrainian border. It was russian military forces that were going to storm the border (see Figure 7).

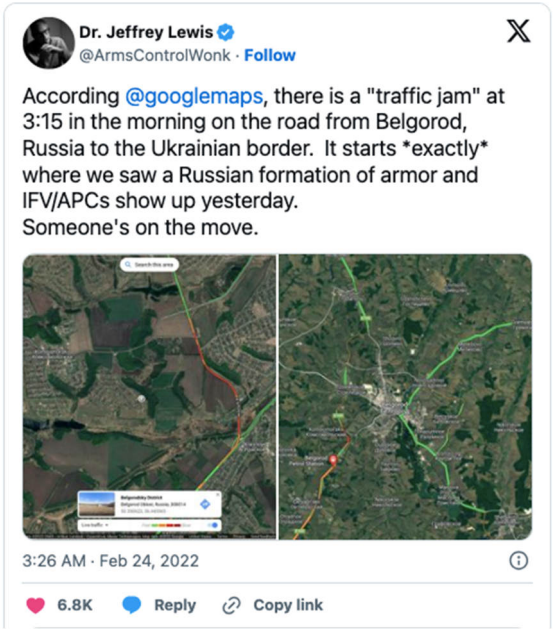

Figure 7. The road near the Ukrainian border on February 24, 2022

Tools such as Flightradar24 and the ADS-B Exchange allowed journalists to track surveillance aircraft operated by the military and its contractors in the days leading up to the invasion and during the ongoing war. This includes a US Air Force RQ-4 Global Hawk reconnaissance drone that was seen on Flightradar24 in Ukrainian airspace, apparently monitoring Donbas on February 24. These same sites were used by the OSINT community to track the movements of private aircraft (see Figure 8). Thanks to the evidence that Ukraine received through OSINT, it was possible to refute the false coverage of events by the russians. As another example, we can take the events in April 2022, namely the appearance of images and videos showing the mass killings of the population in the city of Bucha by russian troops. The city was occupied from February 27 to March 31, 2022.

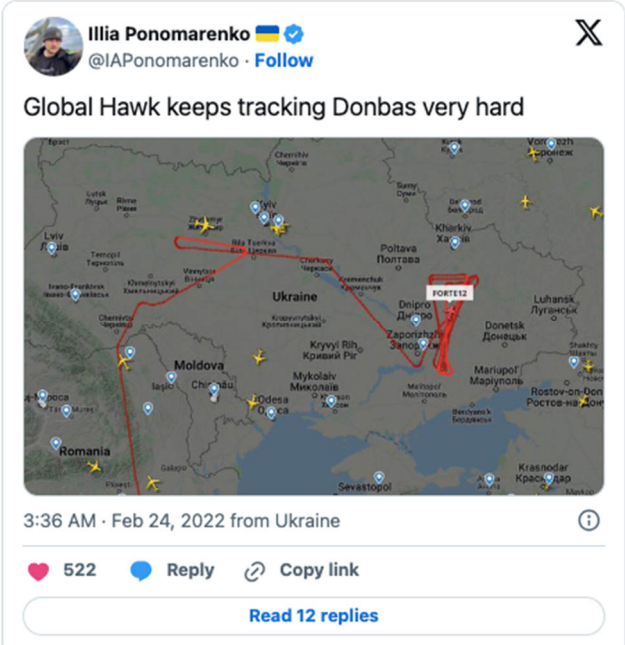

Figure 8. Tracking of surveillance aircraft before the start of the war through the site Flightradar24

However, russia claimed that the killings were actually staged by Ukraine to sway the West to its side. These claims were refuted by satellite images and video analysis, which confirmed that the bodies were present weeks before Ukrainian forces arrived in Buchi. In addition, Ukrainian OSINT analysts are looking for russian military personnel who committed war crimes, based only on the photos in the phones they lost during the escape from Buchi.

These are powerful visual examples of the power of open-source intelligence. The ability to refute russian narratives and maintain an advantage in the arena of international political opinion is critically important for Ukraine. It was thanks to OSINT that we managed to compensate for the quantitative lack of weapons by receiving foreign military aid. Therefore, documenting war crimes has become an area where OSINT has proven successful. The dissemination of images and videos on social networks demonstrates flagrant violations of international law. While the verification itself can be difficult, details such as the insignia of one's own and others' units can be identified for evidence gathering, as can tools such as facial recognition software. Therefore, our specialists are closely related to the search for collaborators, russian agents, and countermeasures against obtaining data about enterprises to take them over. Adherence to international and humanitarian law is currently impossible, but it remains to be seen how exactly evidence obtained from open sources can be used to prosecute war criminals at some point after the war is over.

3. Conclusion

To conclude, we highlighted the critical role of OSINT across strategic, operational, and tactical levels of intelligence gathering. By leveraging advanced technologies such as AI, machine learning, and automated data processing, OSINT demonstrates its potential to transform intelligence methodologies. The study reveals how open-source intelligence can provide crucial insights through satellite imagery, social media analysis, and crowdsourced information, offering unprecedented capabilities in tracking military movements, detecting propaganda, and documenting potential war crimes. Such cases are an important contribution to identifying violations of international law and gathering evidence to bring criminals to justice. We can facilitate a more objective judiciary process and accountability for crimes through OSINT technologies.

The prevalence of OSINT in warfare will not be unique to Ukraine, as the importance of open-source intelligence will continue to grow due to the presence of the Internet and social media in people's daily lives.

References

1. Available online: https://www.euam-ukraine.eu/news/osint-tools-in-the-pursuit-of-justice-in-ukraine/NATO Open Source Intelligence Handbook, (accessed on 07.09.2024).

2. Available online: https://web.archive.org/web/20201107103435/http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf (accessed on 07.09.2024).
3. Intelligence Exploitation of the Internet. Available online: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-005.pdf (accessed on 07.09.2024).
4. NATO Open Source Intelligence Reader. Available online: https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf (accessed on 12.09.2024).
5. Open Source Intelligence Tools And Resources Handbook (2020). Available online: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf (accessed on 12.09.2024).
6. Richard A. Best «Open Source Intelligence (OSINT): Issues for Congress, Congressional Research Service». Available online: https://sgp.fas.org/crs/intel/RL34270.pdf (accessed on 15.09.2024).
7. Admiral William Studeman, «Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community» Available online: https://irp.fas.org/fbis/studem.html (accessed on 15.09.2024).
8. Williams, H., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise. Available online: https://www.rand.org/pubs/research_reports/RR1964.html (accessed on 16.09.2024).
9. Where to use OSINT in your Business? Available online: https://medium.com/@roman_41036/where-to-use-osint-in-your-business-4e9a1b45c19f (accessed on 16.09.2024).
10. Europol sets up OSINT taskforce to support investigations into war crimes committed in Ukraine. Available online: https://www.europol.europa.eu/media-press/newsroom/news/europol-sets-osint-taskforce-to-support-investigations-war-crimes-committed-in-ukraine (accessed on 20.09.2024).
11. Geolocating Tunisian Jihadists in Raqqa. Available online: https://www.bellingcat.com/resources/case-studies/2014/12/19/geolocating-tunisian-jihadists-in-raqqa/ (accessed on 20.09.2024).
12. Locating the Rockets Used During the August 21st Sarin Attacks in Damascus Available online: https://www.bellingcat.com/resources/case-studies/2014/08/10/locating-the-rockets-used-during-the-august-21st-sarin-attacks-in-damascus/ (accessed on 20.09.2024).
13. Available online: InformNapalm. Available online: https://informnapalm.org/ua/ (accessed on 23.09.2024).
14. New data have been established regarding 3 military units of Russia that participated in the aggression against Ukraine. Available online: https://informnapalm.org/ua/vstanovleni-novi-dani-3-vii-chast/ (accessed on 23.09.2024).
15. Tanks for the war in Donbas were supplied by soldiers of the 76th RVB of Russia (PHOTO EVIDENCE). Available online: https://informnapalm.org/ua/tanky-dlia-viiny-na-donbas-postachaly-so/. (accessed on 23.09.2024).
16. Available online: Center "Peacemaker" Available online: https://myrotvorets.center/ (accessed on 25.09.2024).
17. Bellingcat Report - Origin of Artillery Attacks on Ukrainian Military Positions in Eastern Ukraine Between 14 July 2014 and 8 August 2014. Available online: https://www.bellingcat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/ (accessed on 25.09.2024).
18. Bellingcat. Available online: https://www.bellingcat.com/ (accessed on 30.09.2024).
19. MH17 The Open Source Evidence A bell¿ngcat Investigation. Available online: https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf (accessed on 01.10.2024).
20. Ron Penninger, "Operationalizing OSINT Full-Spectrum Military Operations," Small Wars Journal, 14 January 2019, Available online: https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations (accessed on 08.10.2024).
21. Ben Sullivan, "Twitter's the Only Tool You Need for Tracking the Military," Vice News, 24 April 2017. Available online: https://www.vice.com/en/article/wn3g99/twitters-the-only-tool-you-need-for-tracking-the-military (accessed on 11.10.2024).
22. The Ukrainian Foreign Intelligence. Available online: https://www.szru.gov.ua/ (accessed on 12.10.2024).
23. Charlie Winter, John Gallacher and Alexander Harris "Artificial Intelligence, OSINT and Russia's Information Landscape". Available online: https://cetas.turing.ac.uk/sites/default/files/2023-02/cetas_expert_analysis_-_artificial_intelligence_osint_and_russias_information_landscape.pdf