The Growing Weaponization Of Open-Source Information

John P. Ruehl – Independent Media institute

07-04-2024 ~ *Open-source information and intelligence are fueling global participation in the war in Ukraine and other global hotspots, changing how the private sector, the public, and governments influence conflicts.*

Within a day of the June 2, 2024, release of a video documenting the abuse of prisoners of war by a Russian soldier in Ukraine, open-source intelligence (OSINT) researchers had identified the Russian citizen and his involvement in Ukraine going back a decade. Ukrainian officials subsequently sent letters to the International Committee of the Red Cross and the United Nations to document the abuse for potential use in a future criminal trial.

This case is just one example of how OSINT is influencing the war in Ukraine. Online platforms have allowed citizens to broadcast updates to the world, democratizing information and intelligence dissemination. Powerful commercial satellites enable both sides to constantly detect troop and vehicle movements, while georeferencing allows internet users to pinpoint targets through photos and videos. Additionally, social media analysis can track public sentiment and propaganda efforts, providing crucial local and international insights into the psychological nature of the war.

Though the Russia-Ukraine war has shown the latest innovations in wartime OSINT, online platforms and global technologies have increased public involvement in conflicts for years recently. OSINT is being used to shape perceptions of wars, aid in military operations, provide insight into military performances, and expose wrongdoing. Driven by innovations from the private sector, the public, and governments, the growth of OSINT is expected to pose increasing risks to national security and personal privacy.

Foreign maps, news, and propaganda sources have been gathered for centuries to gain insights into the capabilities, preparedness, and strategies of foreign militaries. However, the establishment of the BBC Monitoring Service in 1939 marked a major application of OSINT centralization to gather information about World War II. After the attack on Pearl Harbor in 1941, the U.S. created the Research and Analysis Branch to serve a similar purpose, and as the information age has rapidly progressed since then, OSINT has evolved into a crucial element of modern conflicts.

While Publicly Available Information (PAI) makes up part of OSINT, it also includes commercial data that can be bought or obtained, data about network functions, and algorithms to organize information. Additionally, effective OSINT usage depends on access to data sources, the effectiveness of storing and organizing the data, and reliable and constructive communication to share and debate the findings. Today, individuals thousands of miles away from the front lines play major roles in the fighting, planning, and perception of conflicts, with governments and private actors similarly seeking to exploit OSINT in their own ways.

The Russia-Ukraine War continues to show the critical role of OSINT in modern conflict, building on its application in Ukraine over the past decade. Investigative journalism group Bellingcat used OSINT to expose Russia's involvement in the 2014 downing of Malaysia Airlines flight MH17 over Ukraine and released another report in 2016 documenting Russian artillery attacks against Ukraine. Additionally, OSINT researchers were able to unmask the identities of numerous Russians working for private military and security companies operating in Ukraine from 2014 onward.

In the weeks leading up to the 2022 Russian invasion, organizations like Conflict Observatory amassed large amounts of public and commercially available data to

help identify potential targets and attack points by Russian forces. Hours before Russian forces rolled across the border, Jeffrey Lewis of the Middlebury Institute of International Studies used traffic reports on Google Maps in Russia to indicate Russian action was imminent. Some of the first images of the invasion then came from civilians livestreaming Russian tanks crossing the border.

Since the start of the invasion, OSINT has increasingly favored Ukraine. Social media posts featuring vehicle license plates helped researchersdetermine what types of military vehicles Russia had deployed and where. Viral images and videos of large numbers of destroyed Russian vehicles helped convince Western countries to support more aid to Ukraine, together with other OSINT that has helped expose potential war crimes, debunk Russian claims, and identify war criminals. Meanwhile, Russia banned U.S. social media platforms shortly after the war began, limiting the ability of Russian internet users to coordinate, disrupt, and influence discussions on major global platforms.

Cross-referencing Google Street View photos, viral images and videos, and public satellite data, online researchers have tracked Russian missile launchers. Commercial satellites have helped provide damage assessments of Ukrainian attacks on Russian air bases. Russian soldiers have been targeted through their phones and fitness trackers after connecting to Ukraine's telecoms network, dating apps, geotagged social media posts, and other smartphone features, resulting in fatalities.

A web scraping website, Call Russia, meanwhile collects publicly available data on Russian citizens and allows Russian speakers from around the world to call and talk to them about the war. OSINT relating to the war has also spread to Europe. Bellingcat used OSINT to identify a Russian spy with a fake identity working in Italy in 2022, and Ukrainian OSINT group Molfar subsequently unmasked 167 Russian spies working across Europe in 2023.

Governments were quick to recognize the utility of OSINT in the war and organize it effectively. The U.S. State Department gave immediate support to the Conflict Observatory, and Europol launched an OSINT task force to assist in investigating Russian war crimes. The Ukrainian government created an app for citizens to provide information on military movements and illegal activities, and Ukrainian citizens have been able to direct Ukrainian attacks on Russian positions through their phones.

Nonetheless, Russia has enjoyed some balance in OSINT's application throughout the war. Various sources use OSINT to document Russian and Ukrainian military equipment losses, as well as update daily maps that document troop movements and changes to the frontline. Chatbots continuously scour the internet for data and update receivers with real-time OSINT analysis to identify and alert soldiers to potentially valuable information. U.S. satellite companies are also suspected of providing images to Russian forces, resulting in damaging and deadly attacks that show the vulnerabilities of the West's more open business and internet standards.

Other recent conflicts, particularly in the Middle East, have seen extensive use of OSINT. Throughout the Syrian Civil War, the Live Universal Awareness Map has primarily used social media posts to map current military movements, unrest, destruction, and violence. In 2016, social media users combed through satellite data and located a terrorist camp in the Syrian desert, which was bombed by Russian forces hours later.

OSINT serves as a force equalizer for militant groups with limited access to advanced technologies, and they have drastically increased their use of OSINT in the 21st century. Since the start of the Saudi-led intervention in Yemen's civil war in 2015, Houthi militants have used social media and satellite images to monitor and target the movements of the Saudi-led coalition, though the Saudi coalition has also relied on social media information to target Houthi forces as well. Following the onset of the Red Sea Crisis in late 2023, the Houthis, in coordination with Iran, have used commercially available maritime intelligence services, such as Marine Traffic and ShipXplorer, to track and attack ships through the narrow body of water.

Hamas has employed OSINT against Israel for decades, capitalizing on Israel's open media environment to monitor Israeli policy changes, troop movements, and public sentiment. Since Israel's military bombardment of Gaza began in 2023, the Washington Post's Visual Forensics has mapped Israeli advances using videos, photos, and satellite imagery. Al Jazeera's fact-checking unit Sanad disproved Israel's claim of a Hamas tunnel under al-Shifa Hospital, and additional OSINT proved that Palestinian civilians had been killed by Israeli forces along the safe routes advised by Israel.

Contrastingly, OSINT was used by Israel to challenge reports by Hamas, and repeated by global media outlets, about an Israeli strike that destroyed a hospital.

Bellingcat investigators analyzed footage from the sites of two Hamas attacks in Israel on October 7 to piece together the assault. Additionally, Israeli intelligence actively monitors Hamas on social media, as well as using OSINT in other ways to track Hamas activities.

Outside of active conflict zones, OSINT is also increasingly used as a geopolitical tool. In 1992, the deputy director of the CIA stated that over 80 percent of the agency's analysis was based on OSINT, and the U.S. actively uses OSINT against adversaries and allies. However, the availability and commercialization of data in the West has undermined U.S. global military power. In 2018, for example, the Strava fitness app's user map exposed the positions and movements of U.S. military personnel in Iraq and Syria.

Algorithms can now instantly detect the presence of a ship using global port webcams, while U.S. military aircraft can be tracked on programs like Flightradar24, helping map the U.S. global military presence in real-time. Additionally, WarshipCam and ShipSpotting contain extensive image databases of almost all warships and onboard system configurations. A 2023 report by the University of California's Berkeley Risk and Security Lab stated that China is using various OSINT images of U.S. warships for AI training datasets to build highly detailed computerized images of U.S. and allied vessels.

Additionally, machine learning has made it easy to analyze social media. Lexical analysis, web scraping, and sentiment analysis provide information on language usage and demographics of social media posters. Russia's history of using social media to inflame the U.S. public over divisive issues is well documented, and other states are employing similar tactics to influence the U.S. and Europe. OSINT is also being increasingly used in DNA analysis. China's Beijing Genomics Institute, which works on the Human Genome Project, has amassed millions of people's genomic data for use in studies of populations.

Just as governments and groups use OSINT abroad, they are adapting to its deployment domestically. During the Arab Spring protests in 2010 and 2011, regional governments faced vulnerabilities from protests organized online, with live maps, government atrocities depicted on social media, and other forms of OSINT used. In recognition of this, Beijing acted quickly to pressure foreign companies to remove the HKMap.live app tracking police forces from their platforms and put restrictions on communications during the 2019 and 2020

Hong Kong protests. Western governments may find it challenging to employ such measures amid widespread unrest, resorting instead to tactics such as event barraging by overwhelming the information space with a flood of content to distract and obscure valuable information, misinformation campaigns, trend hijacking, and other methods to undermine OSINT and prevent effective data analysis.

There is also a natural incentive for governments to use OSINT against their populations. By aggregating and analyzing publicly available information and other data, governments can gain valuable insight into citizens' lives, behaviors, and opinions. However, this comes at a significant cost to personal privacy and can make individuals and groups vulnerable to unwarranted surveillance. Law enforcement agencies are increasingly using OSINT in criminal investigations. Moreover, OSINT can be manipulated to shape public opinion, as demonstrated by the "Ghost of Kyiv" during the Russia-Ukraine conflict, which highlighted the potential for OSINT to be hijacked for propaganda purposes.

OSINT is increasingly a major component of the surveillance economy, with companies selling personal and public data for profit. Major names in the OSINT industry include Palantir Technologies, Recorded Future, and Babel Street, among others. These companies, along with numerous smaller firms, continue to drive market growth and innovation. These applications of OSINT extend beyond traditional intelligence gathering, with the increasing sophistication of targeted marketing being one result.

Instances of public misuse of OSINT are widespread, ranging from researchers falsely identifying war criminals to hackers exploiting OSINT for profit. But OSINT has significant positive impacts, including coordinating evacuations and humanitarian aid, alerting civilians to threats, and allowing them to document their experiences that can counter or complement traditional media.

However, much of OSINT continues to be focused on conflict and domestic surveillance, and its capabilities are rapidly expanding as it integrates with machine learning technologies. As OSINT becomes increasingly weaponized and commercialized, the evolving landscape will require increased attention to the ethics of large-scale data accumulation and the threat to personal privacy.

By John P. Ruehl

Author Bio: John P. Ruehl is an Australian-American journalist living in Washington, D.C., and a world affairs correspondent for the Independent Media Institute. He is a contributing editor to Strategic Policy and a contributor to several other foreign affairs publications. His book, *Budget Superpower: How Russia Challenges the West With an Economy Smaller Than Texas'*, was published in December 2022.

Source: Independent Media Institute