Pablo Mathis

Hiding in Plain Sight: The Opportunities and Challenges of Open-Source Intelligence

From analysing the downing of Flight MH17 over Ukraine in 2014 to investigating international crimes committed in the Russia-Ukraine War, open-source intelligence (OSINT) has gained ample media attention. Labelled "the people's panopticon" by The Economist (2021a, title section), OSINT grants citizens unprecedented insights into international relations and conflicts. Moreover, OSINT is set to reshape international justice and investigative journalism.

OSINT for Ukraine

OSINT for Ukraine is a non-profit organisation dedicated to using open-source intelligence to uncover Russian disinformation campaigns and atrocities in Ukraine (OFU, n.d.-a). The organisation has branches in The Hague, Amsterdam, and Berlin (OFU, n.d.-b).

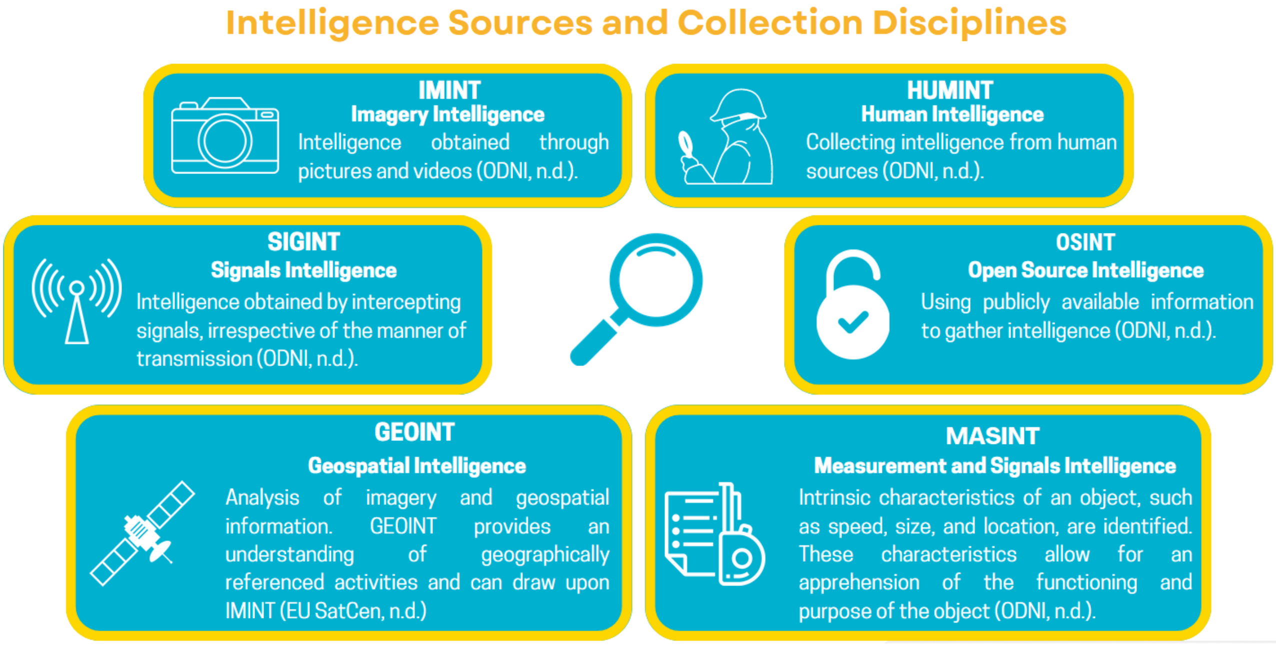
https://www.osintforukraine.com/

This background article draws on personal communication with Deniz Dirisu, chairman of OSINT for Ukraine, to provide an understanding of the methodology, application, and societal debate surrounding OSINT. The ensuing paragraphs present a conceptualisation of OSINT and assess the factors behind the great insights produced by open-source information. Later, to obtain a comprehension of the unique OSINT methodology, the concept of the intelligence cycle will be applied. Beyond investigative journalism, this paper also seeks to provide an understanding of OSINT's application in international justice. Lastly, questions on the accountability of OSINT organisations and governments regarding vital interests are discussed. This paper posits that accountability concerns over vital interests are not unique to OSINT but are as old as democracy itself. The rising prominence of OSINT might thereby fuel a long-overdue debate concerning vital interests.

OSINT: What is in a Name?

The term OSINT entails two aspects: open-source and intelligence. Intelligence is the concept underlying OSINT and can denote a process, product, or organisation. Key to intelligence as a process is the verification and interpretation of information, with intelligence as a product being the result of said process. However, the term can also apply to organisations such as the OFU that carry out and produce intelligence.

What sets OSINT apart from other forms of intelligence is that it relies on openly accessible sources. Openly accessible sources are available to the public and can be used to obtain information through legal means. Nevertheless, grey areas exist: "Take information published online by a hacker or whistleblower. If another party were to use this information to produce intelligence, I would still regard it as OSINT. After all, the information was publicly available," explains D. Dirisu (personal communication, December 13, 2023). Whereas much of the information is obtained freely online, OSINTers may also pay to receive specific information. In these circumstances, the criterion for open access is that the information is still obtained legally and, provided payment, is accessible to everybody. An example of such paid services is the company Satellogic, which provides satellite images to a paying client.



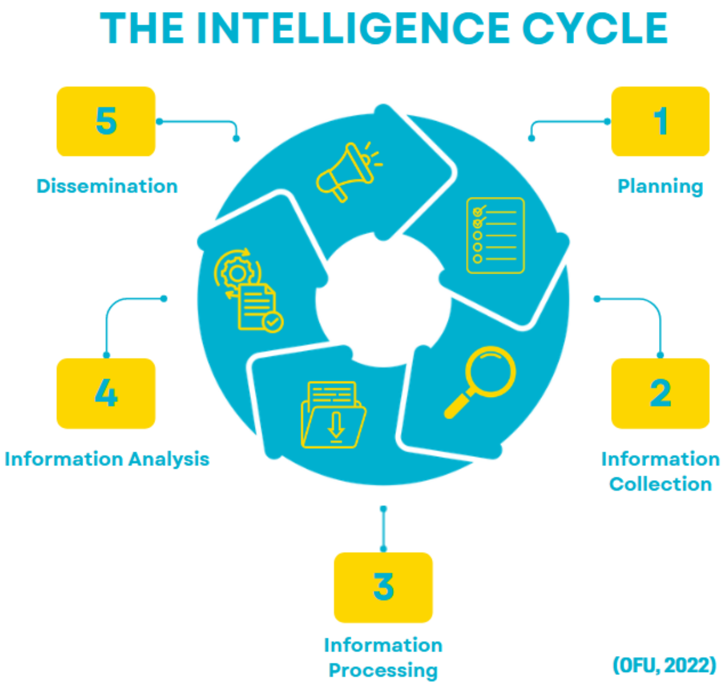
Hiding in Plain Sight: The Power of OSINT

While listening to D. Dirisu, one cannot help but wonder how much is hidden in plain sight. Over the last decade, internet and social media proliferation has led to an exponential increase in information. With this plethora of information and users' obliviousness to what they disclose online, a treasure trove of potential intelligence lies at our fingertips. It comes that although OSINT can be traced back as far as the American Civil War, its increasing prevalence is closely linked to the rise of the internet (Block, 2023).

The breakthrough of OSINT into public conscience arguably came with the downing of Malaysian Airlines Flight MH17 over Ukraine in 2014. Bellingcat, another OSINT organisation, obtained high media attention with its investigations into the accident (Block, 2019). However, OSINT is not limited to investigative journalism and has been employed for military purposes, corporate espionage, and evidence gathering for legal proceedings.

Regarding Russia's full-scale invasion of Ukraine in February 2022, OFU initially saw intense social media coverage. However, D. Dirisu notes that individuals have become more cautious about uploading information on social media: "What we are witnessing in Ukraine is the engagement of two hierarchically organised militaries. As such, commanders can effectively discipline soldiers on their social media usage" (personal communication, October 9, 2023). In addition, Ukrainian officials have urged civilians to be prudent about the sensitive information they reveal on social media. Moreover, changing algorithms at X have impacted the work of D. Dirisu: "With Musk's take over and the decreasing importance of fact-checking at X, disinformation has increased. For us, this means we ought to be extra diligent in using information from X" (personal communication, December 13, 2023).

The Intelligence Cycle: From Information to Intelligence



(OFU, 2022)

Since OSINT is based on openly accessible information, conducting OSINT seems all too easy. But this is not to succumb to the fallacy that information equals intelligence. "If I find a picture of a destroyed tank online, this is not intelligence but open-source information," warns D. Dirisu (personal communication, December 13, 2023). However, open-source information can form an essential part of the intelligence cycle that produces OSINT. The intelligence cycle entails verifying and interpreting information and constitutes the difference between what some deem good and bad OSINT. "Bad OSINT is pure speculation, rushing to conclusions without verification," remarks D. Dirisu (personal communication, December 13, 2023).

The first phase of the intelligence cycle is the planning stage, during which an investigator determines what he is looking for. For OFU's work, investigators ideally have a good command of Russian and Ukrainian. Moreover, detailed knowledge of the country and conflict is beneficial. As D. Dirisu points out, “If you want to find a rat, you must think like a rat” (personal communication, December 13, 2023).

The first stage constitutes the basis for the second stage, in which the OSINTer collects information. IMINT, GEOINT, and SIGINT constitute the main collection methods in OSINT. A primary source of GEOINT is satellite imagery, which can be obtained through free-to-use services such as Google Earth and Google Earth Pro. However, the availability of satellite images can be limited by the stellite’s orbit, meaning the satellite did not photograph a particular area at the time of interest. Resolution constitutes another potential shortcoming of satellite imagery. To identify buildings, a resolution of 10 metres is necessary. Although free satellite imagery providers provide this resolution, challenges augment regarding vehicles and missile or artillery strikes. These require a resolution of 1 metre or less, and humans only become visible at 30 centimetres. Said deficiencies can be addressed by paying companies such as Satellogic to provide higher-resolution images and change their satellites’ orbits. However, obstacles like cloud coverage might remain (D. Dirisu, personal communication, January 10, 2024).

A prominent SIGINT tool is Flight Radar 24. Flight Radar 24 employs a network of receivers that record ADS-B transponder signals to track aircraft. ADS-B transponder signals provide information on an aircraft's identity, altitude, speed, and GPS location (Flightradar24, n.d.). Nevertheless, pilots can turn off their transponders. In such cases, D. Dirisu and his colleagues might rely on VISINT, which planespotters upload online (personal communication, December 13, 2023).

The third stage in the intelligence cycle is information processing. During this stage, information is downloaded, and context is added. “We have to work under the assumption that nothing is obvious. When we download material, the context might be clear to us but not others. Failing to provide context will lead to speculation.”, cautions D. Dirisu (personal communication, January 9, 2023)

The fourth stage includes data verification. “The greatest asset, but also the greatest weakness of OSINT, is exactly that: it is all open source. A post can be uploaded with little regard to authenticity.”, emphasises D. Dirisu (personal communication, October 9, 2023). Methods of verification are ample and used in combination. The investigators can assess the track record of a source and whether it is known to publish authentic information. An investigator will never rely on a single source, cross-referencing all his information. Another method is reverse image searching, allowing analysts to find the earliest version of an image posted online. Employing this tool is particularly relevant in detecting cut or otherwise manipulated content.

The final step of the intelligence cycle is the writing and disseminating of intelligence reports. In this phase, investigators face a crucial dilemma. Intelligence reports ought to balance acknowledging the uncertainty of findings while presenting a specific probability estimate. On the one hand, precise estimates are difficult, as intelligence covers unique events that defy empirical frequencies. On the other hand, a degree of specificity remains necessary (OFU, 2022). "If I say something is possible, it could range from 1 to 99 per cent probability. This uncertainty curtails the value of intelligence", D. Dirisu warns (personal communication, January 9, 2023).

Beyond Investigative Journalism: Legal OSINT

OSINT has gained attention as a tool for investigative journalism. Beyond that, OSINT is employed for legal purposes. "Traditional, boots-on-the-ground fact-finding missions are difficult in active war zones. OSINT can provide a new avenue for prosecuting international crimes.", illustrates D. Dirisu (personal communication, December 13, 2023). Nevertheless, transitioning from intelligence to evidence remains a delicate procedure. For starters, a strict chain of custody aims to prevent tampering with potential evidence. This includes rigorous documentation on where the information is stored, who accessed it, and what analyses were conducted (D. Dirisu, personal communication, October 9, 2023).

Core International Crimes

International crimes are serious violations of international law such as (Rome Statute of the International Criminal Court, 1998):

- Genocide
- War Crimes
- Crimes Against Humanity
- Crimes of Aggression

Another challenge in producing legal evidence lies in the education of legal practitioners. Currently, law students receive little training on the use of OSINT. To this end, D. Dirisu, himself a legal professional, founded the International Crimes Investigation Group. A department of OFU it seeks to bridge the gap between OSINTers and legal practitioners. Together, the International Crimes Investigation Group gathers evidence on international crimes committed during the Russian-Ukrainian war. Later, the evidence is shared with national and international law enforcement authorities (OFU, n.d.-b).

Belling the Cat: Using OSINT Towards Greater Government Accountability

When contemplating the insights OSINT provides citizens, one is reminded of the fable Belling the Cat. In the fable, a group of mice seeks to tie a bell around a cat’s neck to warn them of the cat's presence. Despite meeting approval, the mice cannot find a volunteer to bind the bell on the cat. To some extent, the fable might remind readers of government accountability. A lot is undertaken to hold governments accountable, but efforts can fall short, and citizens remain in the dark. Against this background, OSINT might shed light on hitherto undisclosed government activities. Little surprise, then, that the OSINT organisation Bellingcat lends its name from said fable (The Economist, 2021a).

Given the array of checks and balances, some readers will posit that OSINT is superfluous in democracies. Nevertheless, a point can be made that deception still exists in democracies. Accountability might encourage leaders to cover up failed policies and fearmongers to justify policies. Moreover, deception requires a degree of trust. Trust is more likely between politicians and citizens in democracies. Arguably, citizens are also less informed about foreign than domestic politics, increasing the need to trust government representatives (Mearsheimer, 2011). Deception can further be facilitated by the exclusivity of intelligence, allowing leaders to manipulate the flow of information. A case in point is the 2003 Iraq war. Bush administration officials referred to intelligence reports indicating Saddam Hussein possessed weapons of mass destruction (Walt, 2018). With today’s prevalence of OSINT, these claims could be contested.

OSINT: A Double-Edged Sword

Looking at the 2003 Iraq war, one is encouraged to dive deeper into the annals of history. There, one stumbles upon a nuclear war, averted only by deception: the Cuban Missile Crisis. The US withdrawal of Jupiter missiles from Turkey in exchange for the withdrawal of Soviet missiles from Cuba was long denied by US officials. A case can be made that the Kennedy administration's deception was justified, given fears that the American public would not have accepted such a compromise (Mearsheimer, 2011).

With the proliferation of the internet empowering OSINT, sensitive information might be revealed to the public, endangering international stability (The Economist, 2021b). Against this background, it might be true that "there are different kinds of truth for different people. There are truths for children, truths that are appropriate for students, truths that are appropriate for educated adults … . and the notion that there should be one set of truths available to everyone is a modern democratic fallacy" (Kristol, as cited in Thompson, 2011, para.15). Consequently, are there vital interests for which government accountability should be eased and deception tolerated? And would this mean OSINT is more a curse than a blessing?

Refraining from blatantly rejecting Kristol's quote as undemocratic provides an appreciation of the rationale underlying deception. Kristol's distinction between children, students, and adults reveals that some politicians believe their constituency cannot grasp the complexity of certain affairs. Here, OSINT might close the perceived competency gap between leaders and the public. With OSINT contributing to an enlightened demos, repercussions of disclosing sensitive information to the public will be ameliorated, and incentives to deceive decreased.

Conclusion: The Need for Greater Debate

Above, questions of government accountability regarding vital interests were treated as a matter unique to the rise of OSINT. However, the historical examples presented indicate that this conundrum is not new. It follows that the discussion on OSINT, transparency, and vital interests is not unique but a testimony to an underlying conceptual debate. Which vital interests are so critical that they are best kept secret?

This paper does not provide a definitive answer on vital interests and the role of OSINT. However, this background article can be understood as providing food for thought for a public discourse. Encouraging an open debate goes a long way to resolving outstanding issues on the role of OSINT, government transparency, and vital interests. A discussion of these topics can yield different results. Citizens might opt for complete transparency, handing OSINT organisations a carte blanche. In contrast, deliberation might also restrain the activity of OSINT groups and delineate areas in which government secrecy is condoned. Regardless of the outcome, what matters most is that there will have been a public debate.

References

Block, L. (2019, May 6). *How Bellingcat demonstrates the power of OSINT.* Leidensecurityandglobalaffairsblog. https://www.leidensecurityandglobalaffairs.nl/articles/solving-the-mh17-and-the-skripal-case-how-bellingcat-demonstrates-the-power

Block, L. (2023). *The long history of OSINT*. Journal of Intelligence History. https://doi.org/10.1080/16161262.2023.2224091

European Union Satellite Centre. (n.d.). *What is GEOINT?* https://www.satcen.europa.eu/what-we-do/geospatial_intelligence

Flightradar24. (n.d.). *How flight tracking works.* https://www.flightradar24.com/how-it-works

Mearsheimer, J. J. (2011). *Why leaders lie: The truth about lying in international politics.* OXFORD UNIVERSITY PRESS.

Office of the Director of National Intelligence. (n.d.). *What is intelligence?* https://www.dni.gov/index.php/what-we-do/what-is-intelligence

OSINT for Ukraine. (2022). *Investigation Manual.* https://static1.squarespace.com/static/626ef32886867e5389251d32/t/63d119311021093e2bd79e8a/1674647860219/24_01_2023_investigation_manual.pdf

OSINT for Ukraine. (n.d.-a). *About us.* https://www.osintforukraine.com/about

OSINT for Ukraine. (n.d.-b). *Departments.* https://www.osintforukraine.com/departments

Rome Statute of the International Criminal Court, July 17, 1998, https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf

The Economist. (2021a, August 7). *The promise of open-source intelligence.* https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence

The Economist. (2021b, August 7). *Open-source intelligence challenges state monopolies on information.* https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information

Thompson, C.B. (2011, March 7). *Neoconservatism Unmasked.* Cato Unbound. https://www.cato-unbound.org/2011/03/07/c-bradley-thompson/neoconservatism-unmasked/

Walt, S. M. (2018). *The hell of good intentions: America's foreign policy elites and the decline of U.S. primacy.* Farrar, Strauss and Giroux.