OSINT and the war in Ukraine: workshop summary

Van Puyvelde D.T.N.; Tabarez Rienzi, F.

Universiteit Leiden
Institute of Security and Global Affairs

NWO

Workshop summary

OSINT and the war in Ukraine

Leiden University, Campus Den Haag, 17 May 2024

Damien Van Puyvelde and **Fernando Tabarez Rienzi**

Methodological note

This workshop brought together 15 experts on intelligence and security issues with diverse experiences in academia, the private sector, and government across several Western countries. Their expertise covered: media and journalism; public administration, political science and international relations; criminology; area studies (Russia and its neighbourhood, China); cybersecurity; strategic studies and military affairs; intelligence operations and analysis. The workshop followed the Chatham House (2022) rule, according to which "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." This summary presents the substance of discussions but does not assign points to specific participants. The content follows the overall structure of the workshop, which was divided into five sessions of 60 to 90 minutes.

This workshop was part of 'Open-source research and the war in Ukraine: intelligence for the people by the people?' with project number 406.XS.04.088 of the research programme SSH Open Competition XS pilot 2022-2023 round 4 which is (partly) financed by the Dutch Research Council (NWO).

1. STATE OF THE ART

This session started with a presentation of a literature review produced by the project investigators. Participants were then encouraged to provide feedback on what the review paper covered and did not cover. When discussions pointed out specific literature, the project team conducted a brief follow-up research to add references to this summary paper.

1.1 Semantics

Explicit mentions of "open sources" can be traced to the early twentieth century. Robert David Steele (1992) is one of the first traceable users of the term OSINT. When did specialized individuals and teams (inside and outside government) start to identify as OSINT practitioners themselves? More broadly, why do groups decide to identify or present themselves as OSINT practitioners?

The lack of consensus on definitions limits meaningful discussion and leads to much confusion. Many key concepts remain vaguely defined. Here it is important to consider how institutional interests affect how OSINT is defined (what is excluded or not and why).

1.2 Boundaries of OSINT

OSINT as a discipline: boundaries are not fully clear, consider overlap with SIGINT for example (Weinbaum, Berner, & McClintok 2017).

OSINT and information operations: is the product of hack and leak operations OSINV/T, when does it become and stop to be OSINT? Government-backed actors can hack into systems and then leak data in the public space to influence OSINT coverage. One example is the collaboration of some cyber partisans with Bellingcat to identify GRU officers. Another example is GUR/SBU (Ukraine) information operations through the release of curated audio interceptions on social media. In another instance, Ukrainian hacker collective Cyber Resistance have engaged in hack and leak operations via InformNapalm, who in turn amplify that information with its mass following. How much of OSINF/T is the product of influence or even deception operations (see e.g. Waters 2013)?

Disciplinary boundaries: a vast range of intelligence disciplines from SIGINT to GEOINT rely on publicly available information, and can therefore be at least partly executed outside the realm of secrecy. Possible expressions to convey this reality include: open source SIGINT, open source GEOINT (Hatfield 2024). Or should they be subsumed into a wider "open source" discipline?

1.3 Who does OSINT and what are the implications?

- How and why is OSINT employed by non-state actors? Should some of the work of cyber threat intelligence and cybersecurity companies be considered as OSINT? Consider adding a paragraph on data brokers/miners/data market and software providers in literature review section on "integrating OSINT" (Reviglio 2022; Arango 2023).

- Is the growth of OSINT part of the broader narrative on "surveillance capitalism" (Zuboff 2019)?

- Consider the rise of OSINV collectives, not just Bellingcat but also Citizen Lab before that.
- To what extent do their conceptions/practices differ from government intelligence agencies? How do constraints vary?

1.4 Processing and analysing OSINF/T

- Much of the literature on OSINT focuses on collection and overlooks the role of processing, triangulation (across OSINT sources and methods) and analysis.

- To what extent can artificial intelligence be leveraged to support the production and analysis of OSINF/OSINT? See paper from Alan Turing Institute (Winter, Gallacher, & Harris 2023).

1.5 Uses of OSINT

- **To support court cases:** mention the Berkeley protocol (UNOHCHR 2022); cite some of the legal literature in review paper (Sampson 2017; Letoqueux & Aumaître 2022).

- As a tool for **investigative journalism** (Westcott 2019, 387; Mielcarek 2022; Roumanos 2022), as a teaching tool for journalism (Nelliyullathil, 2020); OSINF and investigative journalism in Russia (Valeeva 2017).

- In academic **research methods**: Scholars working on weapons proliferation (see e.g. Lewis 2018) and radicalisation/terrorism (Pearson 1999) have leveraged digital research methodologies to support their research. However, broader discussions on academic research methods are not keeping up with digital changes (Limonier and Audinet 2022). The digital world has augmented traditional social sciences research methods, for example by opening new opportunities for triangulation (e.g. Charon 2022). Vice versa, further engagement with social scientific research methods could prove useful to OSINT practitioners interested in developing advanced reports. This gap in the literature also concerns the ethics of research methods (for an exception: Lakomy 2023).

- In **government** & in the context of the war in Ukraine: OSINT can yield information and disseminate it in the public space in ways that push for policy change. It can be disruptive by presenting contradictory evidence to what secret sources suggest. It can also corroborate and validate secret information to orient operations.

1.6 The ethics of OSINT

- What are the **privacy risks** posed by the unique insights that emerge once data from multiple openly available sources are combined? Consider CTIVD coverage of this issue in report on automated OSINT (Oerlemans 2022).

- Have OSINT groups and practitioners developed **codes of conduct**? Do they include norms limiting the use of hacked or leaked data?

- Is the use of hacked and leaked (potential illegal, unethical) data/information by OSINT practitioners justified in the pursuit of resistance?

2. HIERARCHY OF OPEN-SOURCE OUTPUTS & DATASET PRESENTATION

The first objective of our research project is to map the range of non-state actors producing open-source intelligence on Russia's war in Ukraine. To achieve this objective, we used an exploratory approach starting on Twitter and expanding when needed to Telegram and other blogs and institutional websites, focusing on outputs produced during the first year of the war. We listed our results in a dataset that quickly reached around 200 profiles. We then reviewed their posts and used an inductive approach to classify them in three main categories.

The second session thus started with a presentation of four main categories of outputs: information, open-source information, open-source investigation, and open-source intelligence. For each category we presented representative and borderline cases, which provided participants with opportunities to question our framework and classification of outputs.

2.1 Methodological remarks

- The **universe of outputs** we focus on **is limited.** First because we started with Twitter. Second, because we focus on outputs that are made accessible online. This overlooks OSINTers who produce on closed platforms, through selective mailing lists, and in government, for example. But it also aligns with a broader overarching goal to open a discussion on the implications of the rise of OSINT on public understanding of contemporary security.

- Should we include GUR in the dataset or just focus on non-state actors? GUR/SBU social media engagement relies on a variety of intelligence-related material, some of which come from secret sources. Activities are also more in line with information warfare rather than open-source investigation/intelligence. Another line of questioning: where to draw the line when non-state actors are largely funded by government and defence industry (e.g. ISW)?

- Should cybersecurity companies and threat intelligence companies' outputs be considered in the dataset?

- Make sure to use a second coder to revisit classification decisions in the dataset independently, then consider measuring **intercoder reliability**.

2.2 Categorization

- Our **categorization** is not neutral and should not be called a typology but a **hierarchy**, following for example the data, information, knowledge, wisdom (DIKW) model. In our case information < OSINF < OSINV < OSINT. OSINT does not necessarily build on OSINF it can also leverage the absence of OSINF to extract value. See for example the Jane's Intelligence Review study gleaning insights from absence of online data to compile a picture of the readiness and operational patterns of a submarine crew (Sutton 2017).

- **Establishing relevance**: why are we categorizing, what is the **use** of this hierarchy? We must **establish relevance**. In this case we are categorizing to put an end to amalgams observers tend to make between raw information and high-grade OSINT products. This can then support research into what it takes to produce high-grade products and make it clear that this is not accessible to all (hence pushing back against arguments that digital change has "democratized" intelligence).

- Is **"objectivity"** a **missing dimension** of OSINF?

- Is **intended audience** for open-source outputs a missing dimension of our framework? The issue here is that this would be assumed in most cases and might not always be clearly identified by the organizations themselves. Here the discussion crystallized about the ISW, their funding model (reliant on defence industry) and possible distortions this funding source could cause on their coverage. This raises the question of the effect of incentives to produce OSINT on the reliability of outputs. If intended audience is defence industry funders and policymakers with specific purposes in mind, then is this valuable information for public consumption?

- Where does **primary versus secondary** source feature within the table? OSINT is always secondary under our definition. Information and OSINF can be either primary or secondary. Should this feature in the categorization?

- Participants seemed to agree that **OSINV (a process) should not be used, and we should favour OSINT (product)**. If our categorization adopts a (narrow) perspective that is too distinct from what observers tend to use (OSINT higher grade than OSINV outputs), then it risks irrelevance. Much of what we consider as OSINV, practitioners and observers would probably call OSINT. A distinction can then be made between low- and high- grade OSINT outputs. OSINT outputs include a dimension of "communication," meaning that information is interpreted for the reader. At the higher end, dimensions such as "actionable" and "requirements" can be used to define a type of high-end output that is a "product" (the use of the term product denotes the way the output is tailored to a consumer's needs).

- Should/to what extent are OSINT methods taken into account into dataset (e.g. geolocation, other)? Some outputs mix straight OSINT work with HUMINT (e.g. Bellingcat 2018 - relies on "confidential Russian sources"). Is this still OSINT? This links back to definitional issues (cf. 1.2 above). Arguably if the source is not publicly accessible then it is not OSINT. Then what to call this output? Note that this case might not be problematic for our dataset, as our codebook makes clear we aim to classify based on the majority of outputs produced by an actor (thus allowing for some exceptions).

- What are the **next steps** and how can we use categorization effectively? For example, should we make a typology of different type of OSINTers/open investigators (as opposed to focusing on outputs)? To what extent can both be amalgamated?

2.3 Value of different types of outputs

- **OSINT is what people make of it.** Value of different types of outputs largely depends on who consumes it. For an intelligence professional, raw information and OSINF can be more valuable than OSINV. In some case **raw information can directly be actionable** and help in targeting individuals, while OSINV cannot. The validation of raw data and information can sometimes be done more quickly, because it relies on metadata created by the platform where it is accessed. Here there are also some limitations to OSINT as it might only provide data for static targeting (less so for dynamic targeting).

  In other situations, raw information and disinformation can have intelligence value, for instance, if the requirement is to track disinformation. OSINT can also be more helpful than other INTS if the requirement is to conduct sentiment analysis. It can also be helpful strictly in combination with other INTs (e.g. as a verification or red teaming mechanism). Thus, the value of outputs depends on the requirement (e.g. targeting, improving understanding of latest trends in the war).

  While we present a hierarchy based on the "quality" of the output in term of how carefully the information is curated and packaged, this does not equate its value to all possible consumers. In this context, actionable can also mean an output, for example a BBC report, informs policy and public understanding. Defining value for the layperson is necessarily based on assumptions and can be problematic. Do we assume the lay reader has clearly defined requirements and know what is valuable information? Is a simple photograph or video enough to satisfy their needs?

- **Value/reliability is not always based on place in the hierarchy**. An unsubstantiated statement can come from a highly reliable account who an insider would know hides another insider or reliable person. So raw information could be very valuable to some well-informed observers and others might completely miss it (e.g. Aurora – lots of primary data?).

3. GRADING OSINT

The third session focused on the effort to grade the reliability and credibility of open-source information, thus raising broader questions about the reliability and credibility of OSINT outputs. Broadly speaking the discussion sought to answer what are the most relevant factors in assessing the quality of OSINT? How to operationalize them?

3.1 Grading frameworks

- The **admiralty code** is most common in Western intelligence agencies but was initially designed only for HUMINT. It is not a good evaluation rubric for OSINT because **not all information is apparent prima facie**.

- **Alternative frameworks** include the KGB system which also considered how the source obtained the information via a third dimension. **Broader frameworks** include ICD 203, CRAAP criteria (Currency, Relevance, Authority, Accuracy and Purpose; Blakeslee 2004); unruly data (Feinberg 2022); Universal Intellectual Standards (Kleinsmith 2020; Elder & Paul 2008).

- In his research on the topic, **Mandel over-relies on a quantitative approach**. The admiralty code scale is **not an interval, it is an ordinal scale**. The distance between A and B can be much bigger than between B and C for example.

- To what extent is grading dependent on requirements and vice versa?

- **Practitioners seem to** prefer **unstructured** grading when evaluating OSINT. Typically, they evaluate **multiple sources** within an OSINT product. **Corroboration** within an OSINT product is done through **data source triangulation**, good OSINT can be corroborated by **method triangulation**.

3.2 Status of a source in OSINT

- Who is the source in news media articles? What is a primary and secondary source in the context of OSINT? OSINT is, by definition, second-hand **information**. The intentions behind it are not clear. These sources cannot be controlled, nor can they be tested. Provenance is often obscure, e.g. dataset with data from mixed origins (for similar claims see Block 2021).

- Telegram data posted on Twitter brings data from the fringe to the centre stage of a debate within a community.

- There is a risk of **echo chamber effect** from the circulation of the same information within an algorithmically enclosed social circle.

3.3 Implications

- The effort to grade raw information is a key dimension to distinguish raw information and intelligence.

- Professionals tend to record a **detailed description of the context and grade on single sources** when they can. Then they triangulate the information (multi sources) and that leads to a finalized product that is higher end.

- **Provenance forensics** is important, so is traceability (archive and assign hash values to ascertain whether a piece of information has been altered in any way once it makes its way through social media communications). Value can then be extracted from disinformation when an altered piece of information is compared to the original. Here the value of (dis)information differs from societal perception of this value.

- Forensic and grading work requires resources and is not always systematically leveraged and institutionalised. Institutionalisation implies a level of traceability/transparency in the use of methods to establish accountability.

- Brandolini's law (also known as the "bullshit asymmetry") holds that: "the amount of energy needed to refute bullshit is an order of magnitude bigger than that needed to produce it."

4 OSINT & THE MEDIA ENVIRONMENT

The fourth session started with a presentation on the evolution of the media landscape and the way it shapes public coverage and perceptions of conflicts. Specific references were made of an experiment in which a team of OSINT practitioners was assembled to produce specific vignettes of the war in Ukraine. The aim was to orient some discussions on the broader environment that enabled the rise of OSINT, and what it takes to produce "high grade" OSINT outputs.

4.1 Participative warfare

- How war is represented in the twenty-first century has fundamentally changed because of smartphone and user-generated content. Each war is mediated in different ways, and this applies to the Ukraine war. OSINT community reshapes the information space, challenging governments to move away from a traditional model based on hierarchy and information access/strict compartmentalization.

- The use of smartphone by civilians to track movements and event to participate in targeting via dedicated apps can make them participants to the war.

- This approach has been leveraged by commanders to find shortcuts in the OODA loop, but also to market their brigade or unit in the public space and project success.

- Western armed forces continue to struggle to adapt to this new information environment (e.g. soldiers' compliance with rules regarding use of smartphone).

4.2 Explaining the rise of OSINT communities

- Western states have **strong civil societies**, **up-to-date technology,** and easy **access to media**, this can explain why OSINT outside the state took off.

- **Other structural factors include:** effect of employment law, privacy laws in specific countries on emergence of communities.

- **Institutionalising OSINT in an academic context requires:**
  - ⇒ Interdisciplinary environment
  - ⇒ leadership support
  - ⇒ freedom to develop niche expertise.

- As the OSINT community grows and diversifies there is an increasing risk of **growing further apart**. For example, there are OSINTers in the national security domain, law enforcement, and technical cybersecurity. Should we seek to **integrate OSINT sub-communities** better? If so, how? What are the **factors** facilitating **integration?**

- To what extent has the community **matured**? Has enough **time** passed to observe **professionalization** in early adopters?

4.3 Epistemic authority & the OSINT community

- "Epistemic authority is authority we ascribe to people in virtue of their favourable relation to epistemic goods such as true belief, rational credence, knowledge, or understanding" (Jäger 2024). This concept is relevant, if not central, to discussions about the overall implications of OSINT for public understanding of contemporary security issues. A variety of online personae refer to and use OSINT techniques or keywords, which conveys forms of authority. How do varying use of terms and practices associated with OSINT shape the information environment? Do some OSINT practices (e.g. geolocating) provide more authority than others?

- How does the OSINT community self-moderate, to out or expel "fakers"? What mechanisms are used to promote or obscure some voices in this community and when are they used?

- To what extent is authority in the OSINT community shaped by credentials more than practices? Some highly followed accounts known for their coverage of the war belong to figures of authorities such as university professors and retired generals. Journalists (who derive part of their authority from their credentials) can also be associated to OSINV techniques which can add credibility to their coverage.

5 LOOKING FORWARD

The workshop closed with an open-ended discussion on issues and angles participants felt we did not sufficiently cover. This was an opportunity to underline the importance of some of the themes that were mentioned earlier and identify new avenues for research and collaboration

5.1 Defining OSINT

- Is the definitional debate really settled? US v European definition?
- Open does not mean accessible.
- Commercially available does not mean legitimately acquired. There are illegitimate markets for data. Should commercial data be considered "open" in OSINT because of the costs?

5.2 OSINT groups as a challenge to the state

- Case of network of former government officials and OSINT community leveraging OSINV to locate and facilitate the exfiltration of Afghan translators not otherwise helped by state agencies, following the "fall of Kabul" (Sylvain 2021). In at least one instance this seems to have put a group in a direct confrontation with a government agency.

- To what extent do autocratic countries have independent OSINT communities? (e.g. Navalny's Anti-Corruption Foundation, etc.) Or are they all mostly co-opted by state organs as proxies?

5.3 The people of OSINT

- What would an anthropology or sociological study of OSINTers look like? For example, Belghith's (2021) conducted over a dozen of semi-structured interviews with OSINTers from nine different organizations. Beyond this study, possible questions to pursue this research strand include:
  - ⇒ Do OSINTers have a coherent identity in agency/country x,y,z?
  - ⇒ What are some of the power dynamics in these social circles? Example of NAFO pushing back against voices that raise questions about pro-Ukrainian coverage of the war. Another example could be to ask how HUMINTers, SIGINTers perceive the rise of OSINTers within a government agency?

- What incentives drive people to product/post OSINF/T?
  - ⇒ Improving v. degrading public understanding (efforts to improve can also degrade)
  - ⇒ Money (ISW following industrial interests?); clickbait?
  - ⇒ Ideology: loyalty to the state ("patriotic OSINTers", see literature on patriotic hackers e.g. Dahan 2013; Harrison Dinniss 2012)
    - Ego/fame
    - Psychology: public interest?

- Morbid fascination, "war porn"?

5.4 Integrating OSINT

- How should the services adapt to the rise of OSINT? What would OSINT **integration look like**? How might integration **differ** depending on the **country** in question? What is the **cost of overlooking** the need to **institutionalise OSINT** (e.g. fragmentation, missing revolution)? And what are the **costs of over-developing it** (e.g. no distinct identity and loss of core identity and unique value developed from HUMINT)?

- How has the **private sector** leveraged the rise of OSINT? How have different private sector actors approached it (e.g. big tech and GAFAM, data brokers, digital cyber security companies, consultants)?
  - ⇒ With the rise of data brokers should we talk about the politics and marketization of data?
  - ⇒ In what ways is the private sector (e.g., FlashPoint, Dataminr, etc.) **disrupting** government OSINT? How should government respond?

5.5 Political economy of OSINF/T

- What would a political economy study of OSINT look like (OSINT is a club good, not a public good).

- **Timeliness** of data and information affects their **market value**. Value of grey dataset decreases over time to the point that grey data becomes openly accessible. More and more data become public over time as they lose actionable value. Conversely, valuable information is made exclusive to paying customers. All data is in some way **'paid for'** (e.g., data produced by users on a free app 'pay' by watching advertisements)?

- Consider also **restricted software** that is permitted only for a select few.

5.6 Ethics and legal limits

- To what extent do **ethical guidelines** limit academic research's ability to leverage OSINT techniques? Do university ethics review systems need to evolve to accommodate digital field investigations?

- Legal boundaries: how do **regulations** like **GDPR** limit what can be collected? What are the legal barriers faced by specific types of investigators? Do private sector researchers (working in banking, or in data brokerage) face the same hurdles as academics, how do they differ, what are the implications?

- Do OSINT **codes of conduct** exist? Can they be compiled and compared systematically? What do they say about controversial issues such as the use of sock puppets, or the use of hacked and leaked data?

- How to balance the projected benefits of data yields v. (privacy) risks?

- Should existing regulations and intelligence oversight mechanisms adapt to rise of OSINT?

5.7 OSINT and (academic) research methods

- **Structuring OSINT research**: **OSINT labs** are emerging in some universities, but we are missing academic research methods handbooks on integrating OSINT within existing (social scientific) disciplines. Digital investigation is already changing social sciences methods. This also raises the question of what research methods we should use to investigate the tradecraft of OSINT(ers)?

- **Making sense of OSINT**: The information space is conflicting and noisy, what are the limits to the interpretability of OSINT? How to distinguish between fact and opinion? Does OSINT reinforce the risk of specific biases?

5.8 OSINT & AI

- What are the implications of AI/LLM for OSINT practices (orientation, collection, processing, analysis, dissemination).

5.9 Professionalization

- What counts as "OSINT expertise?" and therefore who is an OSINT expert? How do we **leverage a wide range of relevant expertise?** Examples of expert professionals/entities are journalists, policymakers, ICRC and HR lawyers, arms control researchers, digital anthropologists.

- OSINT practitioners' **trajectories** is an example of the current **fluidity** of OSINT as a community of practice. This raises broader questions about its professionalization and the rise of standards to define this profession via institutions such as the OSINT foundation, and OSMOSIS.

5.10 So what?

The workshop was partly held to facilitate networking and creating **relations between researchers and practitioners**. What is the **societal importance** of our research? Who is our primary intended **audience**? We want to develop a body of knowledge that can be used by practitioners, academic researchers and students.

References

Arango, S. J. (2023). Data brokers: A benefit of peril to U.S. national security? *Ohio State Technology Law Journal*, *20*(1), 107-138.

Belghith, Y. (2021). *The social structures of OSINT: Examining collaboration and competition in Open Source Intelligence investigations*. Master Thesis, Virginia Tech.

Bellingcat Investigation Team. (2018). Skripal Suspects Confirmed as GRU Operatives: Prior European Operations Disclosed. September 20. https://www.bellingcat.com/news/uk-and-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/

Block, L. (2021, October 25). Definition of a 'source' in OSINT. *BLOCKINT*. https://www.blockint.nl/methods/definition-of-a-source-in-osint/

Charon, P. (2022). De l'exploitation des « traces numériques » en contexte autoritaire : une évaluation de l'apport du renseignement de sources ouvertes aux études chinoises. *Herodote* 186, pp. 99-110).

Chatham House. (2022). *Chatham House Rule*. https://www.chathamhouse.org/about-us/chatham-house-rule.

Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. In D. Hart (Ed.), *ICIW 2013 proceedings of the 8th international conference on information warfare and security* (pp. 51–57). Academic Conferences Limited.

Harrison Dinniss, H. (2012). Participants in conflict—Cyber warriors, patriotic hackers and the laws of war. In D. Saxon (Ed.), *International humanitarian law and the changing technology of war* (pp. 251–278). Koninklijke Brill NV.

Jäger, C. (2024). Epistemic authority. In J. Lackey & A. McGlynn (Eds.), *Oxford handbook of social epistemology*. Oxford University Press.

Lakomy, M. (2023) Open-source intelligence and research on online terrorist communication: Identifying ethical and security dilemmas. *Media, War & Conflict*, 17(1), 23-40.

Letoqueux, H., Aumaître, A. (2022). La contribution de l'OSINT aux enquêtes portant sur des crimes internationaux. *Herodote* 186, pp. 55-66.

Lewis, J. (2018). Snooping on denuclearization. *Arms Control Wonk*. May 11. https://www.armscontrolwonk.com/archive/1205172/snooping-on-denuclearization/

Limonier, K., Audinet, M. (2022). De l'enquête au terrain numérique : les apports de l'OSINT à l'étude des phénomènes géopolitiques. *Herodote* 186, pp. 5-18

Mielcarek, R. (2022). Journalisme: l'enquête en sources ouvertes, entre mirage et opportunité. *Herodote 186,* pp. 43-54.Nelliyullathil, M. (2020). Teaching Open Source Intelligence (OSINT) journalism: Strategies and priorities. *Communication & Journalism Research*, 61.

Oerlemans, J.-J. (2022, February 25). Privacy risks of (automated) Open Source Intelligence (OSINT). *About:Intel*. https://aboutintel.eu/privacy-and-automated-osint/

Pearson, D. (1999).Tracking terrorists through open sources. *Journal of Counterterrorism & Security International*, 6(1).

Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview. *Internet Policy Review*, *11*(3), 1-27.

Roumanos, R. (2022). L'OSINT dans le journalisme: vers une redéfinition des composantes spatiales et temporelles de l'évènement. *Herodote 186,* pp. 31-42.

Sampson, F. (2017). Intelligent evidence: Using Open Source Intelligence (OSINT) in criminal proceedings. *The Police Journal*, *90*(1), 55–69.

Steele, Robert David. (1992). E3i: Ethics, Ecology, Evolution, and Intelligence. *Whole Earth Review*, 74–79.

Sutton, H.I., Social media posts reveal submarine deployments. *Jane's Intelligence Review*. December 7.

Sylvain, C. (2021, August 20). *Open-Source Intelligence and Geospatial Intelligence supporting evacuation of Afghan allies, translators, and U.S. citizens in Afghanistan*. https://quietprofessionalsllc.com/news-events/open-source-intelligence-and-geospatial-intelligence-supporting-evacuations-in-afghanistan/

United Nations Office of the High Commissioner for Human Rights. (2022). *Berkeley protocol on digital open source investigations: A practical guide on the effective use of digital open source and information in investigating violations of international criminal, human rights and humanitarian law*. https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

Valeeva, A. (2017). Open data in a closed political system: Open data investigative journalism in Russia. *Reuters Institute for the study of Journalism, University of Oxford*

Watters, Paul A. (2013). Modelling the effect of deception on investigations using Open Source Intelligence (OSINT). *Journal of Money Laundering Control 16* (3): 238–48. https://doi.org/10.1108/JMLC-01-2013-0005.

Weinbaum, C., Berner, S., McClintok, B. (2017). *SIGINT for anyone: The growing availability of Signals Intelligence in the public domain*.RAND

Westcott, C. (2019). Open source intelligence: Academic research, journalism or spying? In *The Routledge international handbook of universities, security and intelligence studies*. Routledge.

Winter, C., Gallacher, J., Harris, A. (2023). Artificial Intelligence, OSINT and Russia's information landscape, *CETaS Expert Analysis*. https://cetas.turing.ac.uk/publications/artificial-intelligence-osint-and-russias-information-landscape

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile.