ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

https://doi.org/10.5281/zenodo.15229531

THREAT ACTORS PROFILING USING OPEN SOURCE INTELLIGENCE

K.Shwetha[1], Akshitha Shakkeri[2], Somidi Akshay[3], Vadithya Yogender[4], Telugu Venu Gopal[5]

[1] Associate Professor, Dept. of CS, Sri Indu College of Engineering and Technology, Hyderabad,
[2 3 4] Research Student, Dept. of CS Sri Indu College of Engineering and Technology, Hyderabad

Abstract

This article challenges the perception of Open-Source Intelligence (OSINT) as a revolutionary shift driven by the explosion of publicly accessible data. Instead, we argue that the rise of OSINT reflects an evolution of traditional intelligence practices: the collection, processing, analysis and dissemination of vast amounts of information. While the exponential growth of open–source data is reshaping the intelligence landscape, it is neither revolutionizing nor democratizing intelligence. Rather, it is prompting both state and non–state actors to explore how best to integrate OSINT practices and enhance digital literacy within their commu- nities. Core OSINT challenges – information overload, reliability, and legal and ethical concerns – remain consistent with broader intelligence issues. Addressing these challenges provides a foundation for consoli- dating OSINT as a community of practice, and linking it to debates on the disputed role of security expertise in the public debate.

Keywords: digital investigation; open-source intelligence; OSINT; security expertise; intelligence

Introduction

The rapid expansion of online data since the advent of the Internet has greatly enhanced the ability of state *and* non-state actors to collect and analyse openly accessible information on a growing range of security issues, from climate change to terrorism and arms proliferation.[1] Over the past decade, the rise of social media and smartphones equipped with cameras has accelerated this trend.[2] Photos and videos from Russia's war in Ukraine and Israel's invasion of Gaza have flooded social media with vast amounts of data, profoundly shaping public perceptions of contemporary security. This explosion of publicly available data has ushered in what some experts view as a new era of intelligence – the targeting, collection, analysis, and dissemination of to reduce decision-makers' uncertainty.[3] The exploitation of publicly accessible data by intelligence practi- tioners in the public and private sectors, as well as civil society, is often referred to as open-source intelligence (OSINT). Despite the growing academic and professional interest in OSINT, efforts to systematically organise knowledge on its rise and implications for security remain limited.

[1]Hamilton Bean, *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence* (Santa Barbara, CA: Praeger 2011).

[2]Matthew Ford, 'Ukraine, participation and the smartphone at war', *Political Anthropological Research on International Social Sciences*, 4 (2023), pp. 219–47.

[3]David Omand, Jamie Bartlett and Carl Miller, 'Introducing social media intelligence (SOCMINT)', *Intelligence and National Security*, 27:6 (2012), pp. 801–23; Peter Gill and Mark Phythian, *Intelligence in an Insecure World* (Cambridge: Polity, 2018),
p. 5; Heather Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018).

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

This article addresses one central research question: how do experts interpret the rise of OSINT and its implications for contemporary security? To explore this, we combined a comprehensive literature review and a semi-structured discussion with a panel of experts. First, we compiled a bibliography of over 100 publications on OSINT using search queries such as: (OSINT OR 'Open source intelligence') AND security. We applied three selection criteria to narrow our focus on:
(1) academic contributions following a social scientific approach, (2) excluding more technical fields like computer science, (3) ensuring relevance to security studies. From this, we identified 25 key publications, which formed the corpus for an annotated bibliography. Four main debates emerged, on semantics, the spread of OSINT, its integration, and the challenges it poses. This initial foray also highlighted additional areas for exploration, such as the ethics of online investigations. Using a snowball method, we expanded the bibliography to capture a broader spectrum of research and debates (e.g. considering research in law and journalism). To integrate the latest trends in the field of practice, we broadened our search to include select non-academic platforms such as blogs and traditional and social media. These sources proved especially useful in connecting conceptual points to empirical practices, for example, on the ethics of OSINT.[4]

We then presented our initial findings to a panel of 15 security experts from academia, the private sector, and government, representing several Western countries.[5] The panel convened for a one-day workshop in May 2024 under the Chatham House rule to promote candid discussion.[6] The exchange allowed us to confirm and expand our coverage of the literature, test the validity of our main claims, and identify areas requiring further research.[7]

The article is structured around four key themes. The first section addresses definitional issues and their implications. We define open-source intelligence and distinguish it from open-source investigation and information. The second section examines the spread of OSINT from govern- ment institutions to broader communities of practice, arguing that the rise of OSINT reflects an evolutionary process rather than a revolutionary one. Sensationalist claims about OSINT's rev- olutionary potential confuse the availability of open data with the production of intelligence. Producing intelligence requires expert knowledge, analytic skills, and careful coordination – resources that are not available to just anyone. This raises the question of the institutionalisation of OSINT, which is addressed in the third section. Framing of OSINT as a set of practices, we empha- sise the need for digital literacy training over the creation of new organisations. The fourth section addresses three core challenges faced by OSINT practitioners: information overload, reliability, and ethics and regulatory boundaries. These challenges echo well-known issues in intelligence work and provide a sound basis to structure digital literacy training. We conclude by discussing the broader implications of OSINT's rise for security studies, linking the rise of OSINT to broader debates on the proliferation of security actors and expertise beyond the state.

Defining OSINT

The definition and understanding of OSINT are subject to ongoing debate and interpretation. This semantic discussion is important because it delineates the parameters of the field of practice and debates about its emergence, development, and implications on

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

international affairs. Experts agree

[4]Melissa Hanman and Jaewoo Shin, *Ethics in the Age of OSINT Innocence* (Muscatine, IA: Stanley Center for Peace and Security, 2020).

[5]The historical emergence of open-source intelligence practices largely occurred in Global North countries, where most well-established centres of expertise continue to be based. The workshop included one OSINT practitioner from a Global South country, who was affiliated with a European university.

[6]'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.' See Chatham House, 'Chatham House Rule', available at {https://www.chathamhouse.org/about-us/chatham-house-rule}.

[7]Damien Van Puyvelde and Fernando Tabarez Rienzi, *OSINT and the War in Ukraine: Workshop Summary* (The Hague: Leiden University, 2024).

on most of the building blocks of the definition of OSINT, but they disagree on its characterisation as an intelligence discipline.

Political entities on both side of the Atlantic have proposed their own definition of OSINT. The US House of Representatives once defined OSINT as 'intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appro- priate audience for the purpose of addressing a specific intelligence requirement.'[8] This definition presents OSINT as a finalised product. More recently, the European Union has construed OSINT as a practice: 'the practice of collecting and analysing information gathered from open sources to produce actionable intelligence'.[9] Both definitions make a useful distinction between 'raw' pub- licly available information – sometimes also characterised as open-source information or OSINF – and OSINT, which results from a more systematic process of collection, exploitation, and dissem- ination to meet a requirement.[10] Civil society investigative groups like Bellingcat put even more emphasis on this process and now use the term open-source investigation (OSINV) to refer to their work, thus also distancing themselves from government and corporate intelligence practices and products.[11]

Following an academic approach, Coulthart and Nussbaum conduct a systematic review of rel- evant literature to extract the core components of a definition of OSINT. They hold that OSINT is 'legally obtained public or commercial information that has been validated, analysed, and dis- seminated to meet an intelligence requirement'.[12] First, their focus on *legally obtained* information distinguishes OSINT from clandestine or covert intelligence-gathering methods, which intelli- gence practitioners and hackers use to manipulate human and technical sources of information.[13] Yet, in some countries, this legal criterion could rule out the use of data stolen by others and available online.[14] While OSINT does not involve gaining unauthorised access to data in a sys- tem or computer (hacking), defining it as inherently 'legal' risks narrowing our understanding of the diverse sources and methods practitioners employ. For example, OSINT often involves using grey data available online, even when their release was unauthorised.[15]

Second, the information is *public or commercial*. It is public in the sense that it is, in theory, acces- sible to all. This excludes protected sources but does not mean that the information is always freely accessible, hence the reference to commercial information. An important implication of the public availability of the information used to produce OSINT is that it is almost always second-hand.[16] The OSINT Foundation explains: 'for the information to be publicly available, it must have been

[8]US House of Representatives. 2006. H.R.1815– 109th Congress (2005–2006): National Defense Authorization Act for Fiscal Year 2006. 6 January, available at {https://www.congress.gov/bill/109th-

congress/house-bill/1815}. See also Office of the Director of National Intelligence, 'Intelligence Community Directive 301', National Open Source Enterprise (11 July 2006), p. 8.

[9]European Union, 'OSINT: Open-source intelligence', Data.europa.eu (2 May 2022), available at: {https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence}.

[10]Bowman H. Miller, 'Open source intelligence (OSINT): An oxymoron?', *International Journal of Intelligence and CounterIntelligence*, 31:4 (2018), pp. 702–19.

[11]Giancarlo Fiorella, 'First steps to getting started in open source research', *Bellingcat* (9 November 2021), available at {https://www.bellingcat.com/resources/2021/11/09/first-steps-to-getting-started-in-open-source-research/}.

[12]Stephen Coulthart and Brian Nussbaum, 'A definition of open source intelligence', *Open Source Intelligence Lab* (Albany: State University of New York, University at Albany), p. 1.

[13]Thomas P. Carroll, 'The case against intelligence openness', *International Journal of Intelligence and CounterIntelligence*, 14:4 (2001), pp. 559–74.

[14]See for example Bellingcat Investigation Team, 'Inside Wagnergate: Ukraine's brazen sting operation to snare Russian mer- cenaries', *Bellingcat* (17 November 2021), available at: {https://www.bellingcat.com/news/uk-and-europe/2021/11/17/inside- wagnergate-ukraines-brazen-sting-operation-to-snare-russian-mercenaries/}; Bill Toulas, '2easy now a significant dark web marketplace for stolen data', *BleepingComputer* (21 December 2021), available at: {https://www.bleepingcomputer.com/news/security/2easy-now-a-significant-dark-web-marketplace-for-stolen-data/}.

[15]Steven Harris, 'Open source intelligence on the Russian internet', *SANS Open-Source Intelligence Summit* (1 March 2024), available at {https://www.sans.org/presentations/a-practical-guide-to-osint-on-the-russian-internet/}.

[16]Ludo Block, 'A (working) definition of OSINT', BLOCKINT (5 December 2022), available at: {https://www.blockint.nl/ methods/a-working-definition-of-osint/}.

collected, processed, and disseminated by someone else for other purposes'.[17] This point, however, does not always hold true. A practitioner could overtly request information to a source or a forum in ways that are publicly traceable, and this could still contribute to a broader effort to produce OSINT.

Third, there is a broad consensus among experts that the effort to *validate, analyse, and dissem- inate* OSINT distinguishes it from other types of information. Casual observers might associate OSINT with photos of destroyed tanks, which have flooded social media since the start of Russia's war in Ukraine. In the absence of a visible effort to validate the source of such pictures, analyse their meaning in the broader context of this war, and tailor the dissemination of relevant information to the needs of an audience, posting a photo together with its source (e.g. a Telegram channel) is more likely to constitute OSINF.

Fourth, the need for an 'intelligence requirement' to be expressed can help to differentiate OSINT from the outputs produced by hobbyists whose coverage sometimes seems to follow their own interests or what they might assume is in the public interest. In contrast, government agencies, private companies, and mature civil society groups work towards requirements that they or their consumers identify.[18]

Scholars and practitioners debate whether OSINT can or should be considered as a distinct intelligence discipline, on par with human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and geospatial intelligence (GEOINT). Some government intelli- gence professionals[19] contend that OSINT does not qualify as a distinct discipline. Many gov- ernment agencies integrate OSINT into other intelligence disciplines, where it often serves as a foundation to orient and validate more specialised capabilities involving human and technical sen- sors.[20] In practice, integration tends to blur the lines between disciplines.[21] For example, Rae Baker demonstrates the use of publicly available electromagnetic signal data and commercial imagery in her maritime OSINT tutorial.[22] The ability to

blend multiple disciplines and corroborate sources and methods is a hallmark of high-end OSINT. While OSINT investigations might challenge con-ceptual and bureaucratic boundaries, that does not negate the existence and value of OSINT as a specialised field of practice.

Unlike other intelligence disciplines, which are defined by the type of source exploited − such as human or electronic communications − OSINT stands apart by relying solely on non-secret sources. Hatfield defines a secret source as one controlled by a government actor who can restrict access to it.[23] However, this focus on state secrets is problematic, as non-state actors, including ter- rorist groups, also tightly control information about their operations.[24] Additionally, limiting the definition of OSINT to non-secret sources overlooks the extent to which advanced OSINT tech- niques, such as public database exploitation and voicemail retrieval, can challenge the boundaries of state secrecy.[25] A notable example comes from investigative group Bellingcat, which used OSINT techniques to uncover the identities and activities of Russian military intelligence officers involved in the poisoning of Sergei and Yulia Skripal in Salisbury.[26] Many observers likely assumed that only government counter-intelligence officers could achieve such a breakthrough. By combining multi- ple sources and methods, advanced open-source investigations can penetrate state secrets in ways comparable to traditional disciplines.

If 'intelligence is as intelligence does',[27] then OSINT can also be defined by its actions. A large community of researchers and investigators identify their work as OSINT, contributing to its devel-opment as a distinct set of practices. These practices vary widely but are unified by the common challenges of finding, collecting, evaluating, analysing, and disseminating information from open sources. Some well-established practitioners consider OSINT as a distinct intelligence discipline, though one that permeates all others.[28] Critiques may argue that proponents of OSINT as a disci- pline have vested organisational interests, but the same can be said of those who seek to dismiss it. From this perspective, debates over OSINT's definition and classification as an intelligence disci- pline reflect personal trajectories, organisational preferences, and cultural variations, influencing who is included or excluded within communities handling open and classified sources.

[17]OSINT Foundation, *OSINT Definitions* (28 November 2022), p. 3.

[18]Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*.

[19]Mark M. Lowenthal, 'OSINT: The state of the art, the artless state', *Studies in Intelligence*, 45:3 (2001), pp. 273–278 (p. 6); Mark M. Lowenthal, 'Open-source intelligence: New myths, new realities', in Roger Z. George and Robert D. Kline (eds), *Intelligence and the National Security Strategist: Enduring Issues and Challenges* (Washington, DC: National Defense University Press, 2004), pp. 275–8; Miller, 'OSINT: An oxymoron?', p. 717;

Joseph M. Hatfield, 'There is no such thing as open source intelligence', *International Journal of Intelligence and CounterIntelligence*, 37:2 (2023), pp. 1–22.

[20]Williams and Blum, *Defining Second Generation Open Source Intelligence*, p. 7.

[21]Cortney Weinbaum, Steven Berner, and Bruce McClintock, 'SIGINT for anyone: The growing availability of signals intelligence in the public domain', *RAND Corporation* (2017); Hatfield, 'There is no such thing as open source intelligence'.

[22]Rae L. Baker, 'Maritime OSINT: Port analysis', *Rae Baker: Deep Dive* (30 November 2020), available at {https://www.raebaker.net/blog/2020/11/30/maritime-osint-port-analysis}.

[23]Hatfield, 'There is no such thing as open source intelligence', p. 3.

[24]Aaron Brantly, 'Innovation and adaptation in jihadist digital security', *Survival*, 59:1 (2017), pp. 79–102.

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

Our definition of OSINT is deliberately broad to encompass a wide and rapidly evolving range of practices, some overlapping with established disciplines like SIGINT and GEOINT. We define OSINT as a set of practices involving the collection, validation, and exploitation of publicly avail- able data and information to meet informational needs. It qualifies as a discipline because it is grounded in a structured body of knowledge, including established concepts and methods. An active community is engaged in defining related standards, as we illustrate in this article. Viewed this way, investigators and spies practised OSINT long before it was formally named.

The spread of OSINT

OSINT emerged progressively. Intelligence historian Christopher Andrew describes early uses of open sources by decision-makers in Renaissance Venice.[29] Practices – such as consulting newspapers from adversary countries – became more systematic when general staffs and institutionalised military intelligence emerged in the late 19th century. Block identifies two main conditions for the emergence of OSINT practices: the existence of a critical mass of (printed) news available to the public, and the expression of specific informational needs regarding adversaries.[30] One of first public uses of the expression 'open-source intelligence' or OSINT can be traced back to an article former Central Intelligence Agency (CIA) officer Robert David Steele published in a professional journal.[31] In the late 1990s, Steele and Lowenthal – another former CIA officer – published an instructional book on OSINT, discussing sources, collectionmanagement, and integration in all-

[25]See for example Michael Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* (Createspace Independent Publishing Platform, 2010); Rae L. Baker, *Deep Dive: Exploring the Real-World Value of Open Source Intelligence* (Hoboken, NJ: Wiley, 2023).

[26]Bellingcat, 'Full report: Skripal poisoning suspect Dr. Alexander Mishkin, hero of Russia', *Bellingcat* (9 October 2018), available at: {https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr- alexander-mishkin-hero-russia/}.

[27]Mark Stout and Michael Warner, 'Intelligence is as intelligence does', *Intelligence and National Security*, 33:4 (2018), pp. 517–26.

[28]Stephen C. Mercado, 'Sailing the Sea of OSINT in the Information Age', *Studies in Intelligence*, 48:3 (2009), pp. 48–55; Office of the Director of National Intelligence, *The IC OSINT Strategy 2024–2026* (8 March 2024), available at {https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf}.

[29]Christopher Andrew, *The Secret World: A History of Intelligence* (New Haven, CT: Yale University Press, 2018), p. 122.

[30]Ludo Block, 'The long history of OSINT', *Journal of Intelligence History*, 23:2 (2024), pp. 95–109 (p. 98).

[31]Robert D. Steele, 'Intelligence in the 1990's: Recasting national security in a changing world', *American Intelligence Journal*, 11:3 (1990), pp. 29–36 (p. 31).

source analysis and operations.[32] The advent of the Internet opened new opportunities to access data and information, fostering the emergence of a larger community of practice from the mid- 1990s onward. Over a decade later, Michael Bazzell, a former special agent with the Federal Bureau of Investigation, authored one of the first handbooks compiling OSINT techniques, thus facilitating the dissemination of a body of practical knowledge.[33] Changes in the online environment, software, and methodological developments have pushed him to periodically update his hand- book. This is now part of a growing body of contributions and initiatives, such as the Atlantic Council's digital sherlocks programme, that focus on how to do OSINT.[34] These contributions, and the establishment of associations and conferences for OSINT professionals, have played an impor- tant role in consolidating a community of practice that goes well beyond government intelligence agencies.[35]

The open nature of OSINT has facilitated its spread beyond state agencies. Over the past decade, professional communities have increasingly leveraged OSINT. First, security studies scholars have used it to research on issues such as weapons proliferation[36] and terrorist organisations.[37] Second, legal and human rights professionals use OSINF and OSINV to document violations of human rights and provide evidence in investigations and court cases.[38] For example, scholars and interna- tional organisations have published guidelines on using digitally derived evidence in investigating violations of international law.[39] Third, investigative journalists employ open-source investigation techniques to expose corruption and human rights abuses.[40] Groups like Bellingcat have sparked debates about whether OSINT has 'revolutionized' conflict journalism,[41] while educators are exploring how to integrate OSINT into journalism curricula.[42] Open-source university laboratories

[32]Robert D. Steele and Mark Lowenthal, *Open Source Intelligence: Executive Overview* (OSS Academy, 1998).

[33]Bazzell, *Open Source Intelligence Techniques*.

[34]Babak Akhgar, Fraser Sampson, and Saskia P. Bayerl, *Open Source Intelligence Investigations: From Strategy to Implementation* (Cham: Springer, 2016); Giancarlo Fiorella, 'Notes from the digital field: Ethical dilemmas in open source research', *Bellingcat*, (18 September 2023), available at {https://www.bellingcat.com/resources/2023/09/18/notes-from-the- digital-field-ethical-dilemmas-in-open-source-research/}; Digital Forensic Research Lab, *Training + Resources* (2024), avail- able at {https://dfrlab.org/training/}.

[35]OSMOSIS, 'About us' (2024), available at {https://osmosisinstitute.org/about/}.

[36]Christopher Hobbs and Matthew Moran, 'Armchair safeguards: The role of open source intelligence in nuclear prolifera- tion analysis', in Christopher Hobbs, Matthew Moran, and Daniel Salisbury (eds), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities* (Houndmills: Palgrave Macmillan, 2014), pp. 65–80; Jeffrey Lewis, 'Snooping on denuclearization', *Arms Control Wonk* (11 May 2018), available at {https://www.armscontrolwonk.com/archive/1205172/ snooping-on-denuclearization/}.

[37]Megha Chaudary and Divya Bansal, 'Open source intelligence extraction for terrorism-related information: A review',
WIREs Data Mining and Knowledge Discovery, 12:5 (2022), pp. 1–35.

[38]Fraser Sampson, 'Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings', *The Police Journal*, 90:1 (2017), pp. 55–69; Sam Dubberley, Alexa Koenig, and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (Oxford: Oxford University Press, 2020); Hervé Letoqueux and Aurélie Aumaître, 'The contribution of OSINT to the investigation of international crimes', *Hérodote*, 186:3 (2022), pp. 57–68.

[39]Emma Irving, Robert W. Heinsch, and Sabrina Rewald, 'Using the Leiden Guidelines to address key issues in digitally derived evidence', *OpinioJuris* (23 August 2022); Eric Stover, Alexa Koenig, and Lindsay Freeman, *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of*

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law (New York: United Nations, 2022).

[40]Anastasia Valeeva, *Open Data in a Closed Political System: Open Data Investigative Journalism in Russia* (Oxford: Reuters Institute for the Study of Journalism, Oxford University Press, 2017); Manisha Ganguly, *The Future of Investigative Journalism in the Age of Automation, Open-Source Intelligence (OSINT) and Artificial Intelligence (AI)*, PhD Thesis, University of Westminster, 2022.

[41]Glenda Cooper and Bruce Mutsvairo 'Citizen journalism: Is Bellingcat revolutionising conflict journalism?', in Kristin S. Orgeret (ed.), *Insights on Peace and Conflict Reporting* (London: Routledge, 2021), pp. 106–20; Romain Mielcarek, 'Journalism: Open sources investigations, between mirage and opportunity', *Hérodote*, 186:3, (2022), pp. 43–55.

[42]Muhammadali Nelliyullathil, 'Teaching open source intelligence (OSINT) journalism: Strategies and priorities', *Communication & Journalism Research*, 9:1 (2020), pp. 61–73.

are emerging in law schools[43] and security studies programmes,[44] particularly in well-established universities in the Global North. Fourth, OSINT is also foundational to the development of com- petitive intelligence in the private sector.[45] Drawing on research about epistemic communities, the spread of OSINT to these fields can be interpreted as the result of a growing demand for expertise to fill information gaps caused by uncertainty in global affairs.[46] This demand may also explain OSINT's success in attracting significant followings on social media, where users likely share a similar need to address uncertainty.

Today, the term OSINT evokes non-state groups like Bellingcat. Yet we understand little about the wider networks of actors, including government units, civil society groups, private companies, hobbyists, and volunteers, that engage in OSINT and support its proliferation.[47] The field lacks exploratory research into the profiles and trajectories of these practitioners, their interactions and how they form networks across organisational boundaries.

The rise of OSINT has sparked an academic debate over its characterisation. Security studies scholars often question whether the rise of 'new' practices should be construed as an evolution or a revolution.[48] Sebe views OSINT as revolutionary, highlighting the unprecedented breadth and depth of available information, and emphasisng resource abundance and diversity.[49] This 'revolutionary' perspective conflates the availability of open sources and the production of intelligence, which requires technical expertise, coordination, and resources. Williams and Blum take a more measured stance, describing OSINT as entering a new phase thanks to the data yields from Web 2.0 and big data.[50] This aligns well with Block's offer and demand model, which highlights the availability of a critical mass of public information and the articulation of specific informa- tional needs.[51] Based on similar premises, Minas predicts OSINT's indispensability in the current century.[52]

The current OSINT hype has raised its profile in online communities, the media, and even in government circles. Intelligence consumers in government and beyond are now more likely to expect more intelligence, in more detail, and faster.[53] As the OSINT community grows and draws more attention, the need for clear standards to evaluate what constitutes (good) OSINT becomes increasingly evident. Many observers and online personas conflate OSINF with OSINT, the latter requiring a more rigorous process of validation and analysis. Competencies among self-identified OSINT practitioners vary widely, ranging from casual participants to highly skilled teams like

[43]Brianne McGonigle Leyh, Jessica Dorsey, Pinar Yolum, et al., 'UU Open Source Investigations Lab

(OSINT Lab)' (University of Utrecht, 2022), available at {https://teaching-and-learning-collection.sites.uu.nl/project/uu-open-source-investigations-lab-osint-lab/}.

[44]Stephen Coulthart, 'Open Source Intelligence Laboratory (OSI Lab)' (University at Albany, State University of New York, 2024), available at {https://www.albany.edu/cehc/osi-lab#tab-about-}.

[45]Lewis Sage-Passant, 'The security intelligence services of the private sector', PhD diss., Loughborough University (2023). [46]Peter B. Haas, 'Introduction: Epistemic communities and international policy coordination', *International Organization*, 46:1 (1992), pp. 1–35 (p. 3); Iver B. Neumann, and Ole Jacob Sending, 'Expertise and practice: The evolving relationship between the study and practice of security', in Alexandra Gheciu and William C. Wohlforth (eds), *The Oxford Handbook of International Security* (Oxford: Oxford University Press, 2018), pp. 29–40.

[47]Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*, p. 10; Matthieu Suc, 'Ces simples citoyens qui traquent les terroristes', *Mediapart* (18 March 2018), available at {https://www.mediapart.fr/journal/france/180318/ces - simples-citoyens-qui-traquent-les-terroristes}.

[48]Steven Metz, *Strategy and the Revolution in Military Affairs: From Theory to Policy* (New York: DIANE Publishing, 1995); David. V. Gioe, Michael S. Goodman, and Tim Stevens, 'Intelligence in the cyber era: Evolution or revolution?', *Political Science Quarterly*, 135:2 (2020), pp. 191–224.

[49]Marius Sebe, 'OSINT from birth to professionalization', *Univers Strategic*, 3 (2014), pp. 248–261 (p. 248).

[50]Williams and Blum, *Defining Second Generation Open Source Intelligence*.

[51]Block, 'The long history of OSINT'.

[52]Harris Minas, 'Can the open source intelligence emerge as an indispensable discipline for the intelligence community in the 21st century?', *Research paper* 139, (Athens: Research Institute for European and American Studies 2010).

[53]Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*.

Bellingcat.[54] At the lower end of competencies, some individuals merely repost images or videos found online, without verifying their sources. Such practices misuse the OSINT label, lending a false sense of credibility to inadvertently misleading information (misinformation) or convey- ing intentional falsehoods (disinformation) disguised as fact-checking.[55] For example, a social media account with over 500,000 followers falsely claimed a satellite image of clouds and shad- ows over a desert depicted craters caused by Iranian missiles in Israel.[56] In contrast, practitioners with advanced OSINT skills meticulously and visibly validate, process,, and analyse information, for example to geolocate and contextualise an incident. Doing so lends credibility to their claims and authority to their persona.[57] When used in such a manner, OSINT techniques can corrobo- rate or challenge emerging narratives about security issues. To preserve OSINT's integrity as both a methodological approach and a community of practice, it is essential to establish and articulate core standards and competencies. Doing so will not only safeguard the credibility of OSINT but also lay the groundwork for its adoption within governmental, corporate, and non-profit organisations.

Integrating OSINT

The rise of OSINT is reshaping the information environment, compelling public and private organ- isations to reevaluate traditional intelligence practices that emphasise information control and compartmentalisation. In information-centric sectors, institutions that overlook OSINT risk miss- ing crucial opportunities to broaden their sources and modernise their methods. OSINT's growing prominence has prompted some Western intelligence communities to clarify their strategies for integration while reaffirming distinct contributions to decision-makers and the public.[58] However, an over-reliance on OSINT carries the risk of eroding expertise in core disciplines like HUMINT and SIGINT, which remain central to the identity and effectiveness of government intelligence agencies.[59]

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

The challenge lies in finding ways to integrate OSINT methods and competencies without compromising the broader intelligence ecosystem.

Integrating OSINT sources and methods poses challenges at three levels: community, organisa- tion, and individual. Looking at the US intelligence community, Amy Zegart suggests creating an independent agency dedicated solely to OSINT,[60] replacing the Office of the Director of National Intelligence's Open Source Enterprise.[61] She argues that specialisation would drive innovation. This reflects ongoing debates, in the United States and beyond, about whether OSINT should be centralised within a single agency or decentralised across various organisations, directorates, and units. A more authentic community approach would promote the development of OSINT competencies well beyond the boundaries of a single government entity.[62]

At the organisational level, the integration of OSINT into government agencies underscores its value as a complementary tool rather than a substitute for more established intelligence methods.

[54]Dan Lomas, 'The death of secret intelligence? Think again', *RUSI* (5 July 2023), available at {https://rusi.org/explore-our-research/publications/commentary/death-secret-intelligence-think-again}.

[55]Alistair Coleman, 'Analysis: How fake fact-checkers spread Ukraine war disinformation', *BBC* (7 July 2022), available at {https://monitoring.bbc.co.uk/product/c203ld1d}.

[56]Manisha Ganguly, post, *X* (15 April 2024), available at {https://x.com/manisha_bot/status/1779832793880494272}.

[57]Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*, p. 9.

[58]Dutch Review Committee on the Intelligence and Security Services, *Review Report – Automated OSINT: Tools and Sources for Open Source Investigation* (22 December 2021); Office of the Director of National Intelligence, *The IC OSINT Strategy 2024–2026*, available at {https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf}.

[59]Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*, p. 11.

[60]Amy Zegart, 'Open secrets: Ukraine and the next intelligence revolution', *Foreign Affairs* (20 December 2022), available at {https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart}.

[61]Previously Open Source Center, see Hamilton Bean, 'The DNI's Open Source Center: An organizational communication perspective', *International Journal of Intelligence and CounterIntelligence*, 20:2 (2007), pp. 240–57.

[62]Jason Parry, 'Open source intelligence as critical pedagogy; Or, the humanities classroom as digital human rights lab', *Interdisciplinary Humanities* (2019), pp. 109–16.

Despite its growing prominence in investigating security incidents, OSINT is unlikely to funda- mentally challenge the enduring importance of secret intelligence in shaping decision-making.[63] OSINT tends to deliver the most value when combined with other disciplines.[64] This reflects the principle that all-source intelligence, which allows for corroboration across multiple methods, is more reliable than single-source approaches. In mature organisations, OSINT is systematically cross-referenced with other intelligence sources, which professionals process and analyse to orient intelligence agencies and inform decision-makers.[65]

This integration process, however, raises critical questions about structure and flexibility. Dover argues for the establishment of internal OSINT teams,[66] while Lahneman advocates a more flexible approach, delegating specific tasks to a trusted network of contractors.[67] This flexibility reflects the reality that non-state actors tend to have fewer security, organisational, and legal constraints that can limit OSINT activities.[68] Moreover, as the private sector owns and brokers much of the data critical to OSINT investigations, governments depend on partnerships with external entities to access data.[69]

The debate over whether to insource or

outsource OSINT capabilities overlaps with discussions on crowdsourcing, where the public is directly asked to help fulfil informational needs.[70] Van der Meulen highlights the challenges faced by Dutch military intelligence in adopting this method,[71] raising questions about its suitability for government agencies. A promising line of research would examine how organisational culture influences the propensity, ability, and integration of OSINT practices and partnerships. Most research on OSINT has focused on state capabilities, despite its importance in the private sector, and non-governmental organisations. Lewis Sage-Passant notes that private-sector intelligence gathering often relies on open sources.[72] Additionally, OSINT prac- tices are accessible to violent non-state actors like Hamas, which have used them to support their targeting efforts against the Israeli Defense Forces.[73] The panel of experts we assembled agreed that how this broader range of non-state actors integrate OSINT remains an underexplored area of research.[74] While not extensively studied, we can hypothesise that groups like Bellingcat suc- ceed because they leverage global and diverse networks that grant them direct access to incident sites, and sources and methods that are not easily developed by more structured government or corporate bodies. If this decentralised, creative approach is a key driver of OSINT's success, the establishment of a centralised government agency dedicated to OSINT could undermine some of its key strengths by introducing rigid frameworks that limit flexibility, innovation, and access to networks of supporters.

Institutional design alone has limited impact if there is no existing inclination towards OSINT. This brings us to a third level of analysis: the individual. Psychologists Pedersen and Jansen show that people tend to place more confidence in secret information than in open sources.[75] Gentry notes that analysts are likely to avoid OSINT if it conflicts with their preferences.[76] Such

[63]Lomas, 'The death of secret intelligence?'.

[64]Brett Miller, 'Evolution of intel: How valuable is OSINT?', *Public Safety* (24 July 2015).

[65]Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), pp. 42–4; John Nomikos, 'The role of open sources in intelligence', *International Security Research and Intelligence Agency* (15 January 2006); Christopher Eldridge, Christopher Hobbs, and Matthew Moran, 'Fusing algorithms and analysts: Open-source intelligence in the age of 'big data', *Intelligence and National Security*, 33:3 (2017), pp. 391–406.

[66]Robert Dover, 'Adding value to the intelligence community: What role for expert external advice?', *Intelligence and National Security*, 35:6 (2020), pp. 852–69.

[67]William J. Lahneman, 'The need for a new intelligence paradigm', *International Journal of Intelligence and CounterIntelligence*, 23:2 (2010), pp. 201–25.

[68]See for example Florian Schaurer and Jan Störger, 'The evolution of open source intelligence (OSINT)', *International Relations and Security Network* (ETH Zurich, 2010).

[69]Steven J. Arango, 'Data brokers: A benefit or peril to U.S. national security?', *Ohio State Technology Law Journal*, 20:1 (2023), pp. 107–38; Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*, p. 3.

[70]Steven A. Stottlemyre, 'HUMINT, OSINT, or something new? Defining crowdsourced intelligence', *International Journal of Intelligence and CounterIntelligence*, 28:3 (2015), pp. 578–89.

[71]Emma Van der Meulen, 'Madness/wisdom of crowds: An exploratory case-study on crowdsourcing as a method for intel- ligence gathering within the Dutch Defence Intelligence and Security Service (DISS)', Master's diss., Netherlands Defence Academy (2022).

[72]Sage-Passant, 'The security intelligence services of the private sector', p. 156.

[73]Netanel Flamer, 'The enemy teaches us how to operate': Palestinian Hamas use of open source intelligence (OSINT) in its intelligence warfare against Israel (1987–2012)', *Intelligence and National Security*, 38:7 (2023), pp. 1–18.

[74]Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*.

tenden- cies suggest that some analysts might neglect or delegate OSINT tasks, undervaluing its potential. Addressing these biases is essential. Familiarising personnel with the value of OSINT could also bring additional benefits. For example, Glassman and Kang find that OSINT collection introduces intellectual puzzles that foster alternative ways of thinking,[77] akin to the advantages of some struc- tured analytic techniques.[78] A practical recommendation, then, is to adapt training programmes to emphasise OSINT's utility rather than creating dedicated units.[79] This strategy aligns with broader efforts to enhance digital literacy while also addressing critical challenges in today's information environment.[80]

Challenges

The main challenges facing OSINT practitioners mirror those confronting traditional intelligence professionals, namely information overload, reliability, and ethical and regulatory issues.[81] First, information overload refers to the overwhelming volume of data and information available for collection and exploitation.[82] This issue has long been recognised, as seen in intelligence failures like the 1941 surprise attack on Pearl Harbor.[83] The digital age has exacerbated this challenge, with vast amounts of data now readily available. Arno Reuser, who helped to establish an early OSINT capability in the Dutch military intelligence and security service, proposes a design solution by reframing and integrating the OSINT process.[84] More operational solutions include develop- ing software to help analysts discover, filter, and analyse large datasets.[85] These efforts intersect with growing interest in using artificial intelligence (AI) to automate the processing and analysis of (open-source) information, offering a potential path to mitigating information overload.[86] As

[75]Tore Pedersen and Pia Therese Jansen, 'Seduced by secrecy – perplexed by complexity: Effects of secret vs open-source on intelligence credibility and analytic confidence', *Intelligence and National Security*, 34:6 (2019), pp. 881–98.

[76]John A. Gentry, 'Favorite INTs: How they develop, why they matter', *Intelligence and National Security*, 33:6 (2018), pp. 822–38.

[77]Michael Glassman and Min J. Kang, 'Intelligence in the Internet Age: The emergence and evolution of open source intelligence (OSINT)', *Computers in Human Behavior*, 28:2 (2012), pp. 673–82.

[78]Stephen Coulthart, 'Why do analysts use structured analytic techniques? An in-depth study of an American intelligence agency', *Intelligence and National Security*, 31:7 (2016), pp. 933–48.

[79]Ardi Janjeva, Alexander Harris, and Joe Byrne, *The Future of Open Source Intelligence for UK National Security* (RUSI Occasional Paper, 2022).

[80]Ahmed Maati, Mirjam Edel, Koray Saglam, Oliver Schlumberger, and Chonlawit Sirikupt, 'Information, doubt, and democracy: How digitization spurs democratic decay', *Democratization*, 31:5 (2023), pp. 922–42.

[81]Peter Jackson, 'On uncertainty and the limits of intelligence', in Loch K. Johnson (ed.), *Oxford Handbook of National Security Intelligence* (Oxford: Oxford University Press, 2010), pp. 452–71; Gill and Phythian, *Intelligence in an Insecure World*, chapter 6.

[82]Arthur S. Hulnick, 'The downside of open source intelligence', *International Journal of Intelligence and CounterIntelligence*, 15:4 (2002), pp. 565–79; Eldridge, Hobbs, and Moran, 'Fusing algorithms and analysts'; Miller, 'Evolution of intel'.

[83]Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), p. 3; Erik Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), pp. 29–46.

[84]Arno H. P. Reuser, 'The RIS open source intelligence cycle', *Journal of Mediterranean and Balkan Intelligence*, 10:2 (2017), pp. 29–43.

[85]Eldridge, Hobbs, and Moran, 'Fusing algorithms and analysts'; Line C. Pouchard, Jonathan M. Dobson, and Joseph P. Trien, 'A framework for the systematic collection of open source intelligence', *Association for the Advancement of Artificial Intelligence* (March 2009).

[86]Dutch Review Committee on the Intelligence and Security Services, *Review Report – Automated OSINT*; Charlie Winter, John Gallacher, and Alexander Harris, 'Artificial Intelligence, OSINT and Russia's information landscape', *CETaS*

advanced data analytics and AI technologies become increasingly central to processing openly available data, a growing divide is likely to emerge. Well-resourced entities, such as govern- ment agencies and private companies, will benefit from access to cutting-edge software, while groups with limited resources, including civil society organisations and hobbyist investigators, may struggle to keep pace. This disparity raises questions about equitable access to technological advancements, and its implications for the broader OSINT ecosystem and information landscape.[87] Second, reliability – the extent to which data consistently and accurately informs analysis –

is a major concern. Open sources are especially vulnerable to intoxication, where adversaries intentionally spread false information to deceive OSINT practitioners and the public.[88] This issue has become more pronounced during Russia's war in Ukraine, which has seen a surge in strategic communication through press releases, orchestrated leaks, and disinformation campaigns.[89] The fog and noise of war complicate efforts to provide a reliable picture of ongoing events. Optimist voices explore how OSINT can help clear the 'fog of war' by dispelling false narratives arising from both sides.[90] Conversely, Schrijver examines how Ukrainian intelligence services have leveraged selectively disclosed protected information on social media to highlight Russian actions and shape public perceptions.[91]

A promising line of research focuses on developing methods to evaluate the reliability of open- source information. Campbell proposes a metric for assessing the legitimacy of content created by OSINT users on Twitter (now X), with questions tied to three types of legitimacy: output, normative, and pragmatic.[92] Digital investigator Aric Toler outlines techniques for verifying and authenticating user-generated content, addressing concerns over OSINT's reliability.[93] Methods like establishing provenance, time, and location through digital tools – such as commercial satellite imagery and reverse image searches – can reduce doubts about authenticity. As the OSINT com- munity matures, it is consolidating best practices and seeking standardisation.[94] However, OSINT alone is unlikely to consistently achieve the reliability offered by more robust approaches that rely on corroboration across the broader spectrum of intelligence disciplines.

Tackling information overload and evaluating the reliability of data requires competencies. The competencies and resources that separate OSINT experts from hobbyists and casual Internet users deserve more scholarly attention. Extensive subject knowledge is crucial for understanding and pri- oritising information on complex security developments.[95] Experience and familiarity with sources

Expert Analysis (2 February 2023), available at {https://cetas.turing.ac.uk/publications/artificial-intelligence-osint-and- russias-information-landscape}.

[87]The authors would like to thank reviewer 1 for suggesting this point.

[88]Hulnick, 'The downside of open source intelligence'; Nomikos, 'The role of open sources in intelligence'.

[89]Illia Varzhanskyi, 'Reflexive control as a risk factor for using OSINT: Insights from the Russia–Ukraine conflict',
International Journal of Intelligence and CounterIntelligence, 37:2 (2024), pp. 419–49.

[90]Hannah van Beek and Sebastiaan Rietjens, 'Open-source intelligence in the Russia–Ukraine war', in Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens (eds), *Reflections on the Russia–Ukraine War* (Leiden: Leiden University Press, 2024), pp. 57–76.

[91]Peter Schrijver, 'Beyond counterintelligence: Understanding the SBU's social media outreach on Telegram during wartime', *Intelligence and National Security*, 39:3 (2024), pp. 525–38; Peter Schrijver, 'The wise man will be master of the stars'. The use of Twitter by a military intelligence service in wartime: The case of the GUR', in Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens (eds),

Reflections on the Russia–Ukraine war (Leiden: Leiden University Press, 2024), pp. 77–95.

[92]Adam Campbell, 'Legitimate actors or security concern? How OSINT hobbyists are changing the nature of conflict', Master's diss., Charles University (2022), pp. 44–50.

[93]Aric Toler, 'How to verify and authenticate user-generated content', in Sam Dubberley, Alexa Koenig, and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (Oxford: Oxford University Press, 2020), pp. 185–227.

[94]Miguel Fernandez, Alan Millington, Mark Monday, and Emil Sarpa, *Elementary … The Art and Science of Finding Information: Achieving More 'Knowledge Advantage' through OSINT* (Saint Petersburg, FL: Booklocker, 2019); Sam Dubberley, Alexa Koenig, and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (Oxford: Oxford University Press, 2020).

[95]Robert W. Pringle, 'The limits of OSINT: Diagnosing the Soviet media, 1985–1989', *International Journal of Intelligence and CounterIntelligence*, 16:2 (2003), pp. 280–9.

also enable analysts to better discern between true and false information.[96] In this sense, OSINT demands skills and resources that are not easily acquired or universally available. The rise of OSINT is not 'democratising intelligence'.[97] Even highly skilled experts can struggle to effectively inter- pret and contextualise open-source information, particularly when tasked with analysing regions or topics outside their expertise. The growing importance of AI tools to process and analyse vast amounts of openly accessible data, and the high costs associated with advanced capabilities in this domain, also suggest that high-end OSINT capabilities are not easily accessible to a broad audience. Third, openly available data, information, and intelligence can harm individuals by violating their privacy or scapegoating them. OSINT requires careful ethical consideration. Gibson high- lights how social media exhibitionism and unrestricted data access blur the lines between public and private spheres, complicating ethical considerations in OSINT activities.[98] Hribar and col- leagues identify legal grey areas in advanced OSINT techniques, noting that government agencies can exploit these to broaden their collection targets and the types of information they collect, potentially infringing on privacy without technically breaking laws.[99] Ronn and Soe similarly warn against the unethical use of social media by intelligence agencies, stressing the violation of privacy rights in public online spaces.[100] These perspectives emphasise the urgent need for communi- ties and organisations to develop clear ethical guidelines and regulations to ensure responsible open-source investigations.

As OSINT practices continue to evolve, incorporating new methods and developing new capa- bilities, adapting regulations and oversight mechanisms becomes increasingly important. The General Data Protection Regulations, for instance, impose strict guidelines on privacy and secu- rity, limiting what data can be collected and for how long it can be kept.[101] Continuing scrutiny is essential to ensure that current regulations adequately address potential harms and are properly implemented and enforced. Regulatory efforts are not limited to supranational organisations or national governments – the OSINT community also has a role to play. The OSINT Foundation, for example, has developed a code of conduct that addresses controversial practices like the use of sock puppets (fake social media accounts) and hacked and leaked data.[102] Scholars, too, can play a role in shaping the normative foundations of OSINT by developing ethical frameworks to guide its practices, including in areas such as social media intelligence.[103] These contributions can help address concerns about the potential misuse of OSINT in sensitive contexts. However, the credibility and utility of normative

frameworks depend heavily on the presence of accountability mechanisms which can incentivise compliance and deter deviations from shared standards.

Further research is needed to explore two key dimensions of accountability in the OSINT domain. First, the extent to which OSINT groups like Bellingcat can contribute to the democratic accountability of government (intelligence services) – by making their activities more transparent to accountability bodies such as parliament, courts, specialised oversight bodies, the media, and the public – remains underexamined. Second, there is a need to investigate how OSINT practition- ers across public, private, and civil society sectors are themselves held accountable for their actions and outputs. Addressing these gaps is essential to foster a trustworthy OSINT ecosystem.

[96]Hulnick, 'The downside of open source intelligence'.

[97]David V. Gioe and Ken Stolworthy, 'Democratised and declassified: The era of social media war is here', *Engelsberg Ideas* (24 October 2022), available at {https://engelsbergideas.com/notebook/democratised-and-declassified-the- era-of-social-media-war-is-here/}.

[98]Stevyn D. Gibson, 'Exploring the role and value of open source intelligence', in Christopher Hobbs, Matthew Moran, and Daniel Salisbury (eds), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities* (Houndmills: Palgrave Macmillan, 2014), pp. 9–23.

[99]Gasper Hribar, Iztok Podbregar, and Teodora Ivanuša, 'OSINT: A "grey zone"?', *International Journal of Intelligence and CounterIntelligence*, 27:3 (2014), pp. 529–549 (p. 539).

[100]Kira V. Rønn and Sille Obelitz Søe, 'Is social media intelligence private? Privacy in public and the nature of social media intelligence', *Intelligence and National Security*, 34:3 (2019), pp. 362–78.

[101]General Data Protection Regulation, 'GDPR Compliance Checklist', GDPR.Eu (2024), available at {https://gdpr.eu/ checklist/}.

[102]OSINT Foundation, 'Statement of principles' (18 March 2024).

[103]Omand, Bartlett, and Miller, 'Introducing social media intelligence'.

Conclusion

There is an emerging consensus on defining OSINT as a process involving the collection, analysis, and dissemination of information from publicly or commercially available sources. This process distinguishes OSINT from 'raw' open-source information, emphasising the rigorous validation and analysis required to turn data into actionable intelligence. Experts broadly agree that OSINT now plays a foundational role in guiding information collection and analysis across various fields. They also highlight three key challenges – information overload, reliability, and ethical and regulatory considerations – that provide a foundation to consolidate core OSINT competencies and develop relevant training.

One point of contention is whether OSINT should be classified as a distinct intelligence disci- pline or as a facet of existing intelligence methods. This debate has significant policy implications for how organisations can most effectively incorporate OSINT capabilities and adapt to the ever- growing volume of open-source data. Some view OSINT's rise as revolutionary, calling for the creation of specialised government agencies dedicated solely to its exploitation. However, much of the evidence indicates that the emergence of OSINT has been more evolutionary, developing progressively alongside other intelligence and digital investigation methods. This suggests that information and digital literacy training might be more important for leveraging OSINT than the creation of dedicated organisations.

Despite OSINT's growing importance, several areas remain underexplored. One

key question is what factors have driven its proliferation over the past few decades. While technological advance- ments are often considered as the primary catalyst, sociological factors – such as career trajectories and networks of acquaintances – have likely also played a significant role in shaping its expan- sion.[104] Investigating the sociology of OSINT could provide valuable insights into broader debates, on the motivations behind digital activism,[105] and the influence of epistemic communities in spreading security knowledge, practices, and discourses.[106]

Second, and relatedly, further research is needed to explore how OSINT is reshaping the role of expertise in security affairs. The rise of OSINT has contributed to the proliferation of security actors and practices beyond the state.[107] While this proliferation does not render the state obsolete, it challenges public authorities to adapt their roles to harness external capabilities.[108] Notably, the increasing involvement of companies and civil society in supporting government agencies requires adaptations in oversight mechanisms to ensure that reliance on external or emerging capabilities does not create new accountability gaps.[109]

The growing prominence of OSINT on social and traditional media also contributes to shaping security perceptions.[110] OSINT practitioners leverage emerging investigation techniques – often relying on striking visual evidence – to make authoritative claims about security affairs.[111] In doing so they act as 'influencers', actively contributing to the construction of contemporary security nar- ratives.[112] However, these techniques are not infallible, and the information and knowledge OSINT practitioners convey can raise critical concerns. A discursive perspective could therefore exam- ine how the rise of OSINT shapes specific understandings of security. In one notable anecdote, a senior Western intelligence official reported that a policymaker asked why they first learned about an emerging security issue from Bellingcat rather than the designated government agency.[113] This example underscores the growing authority of OSINT expertise in influencing policy perceptions, even among government officials. What, then, are the broader implications of the rise of OSINT on the security discourse? In recent years, the Western OSINT community has focused predominantly on threats posed by Russia. To what extent does this

[104]Van Puyvelde and Tabarez Rienzi, *OSINT and the War in Ukraine*, p. 12.

[105]Michael Dahan, 'Hacking for the homeland: Patriotic hackers versus hacktivists', in Doug Hart (ed.), *ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security* (Denver, CO: Academic Conferences Limited, 2013), pp. 51–57; Jordana J. George and Dorothy E. Leidner, 'From clicktivism to hacktivism: Understanding digital activism', *Information and Organization*, 29:3 (2019), pp. 1–45.

[106]Christian Bueger, 'From expert communities to epistemic arrangements: Situating expertise in International Relations', in Maximilian Mayer, Mariana Carpes, and Ruth Knoblich (eds), *International Relations and the Global Politics of Science and Technology* (Wiesbaden: Springer, 2014), pp. 39–54 (p. 40); Hager Ben Jaffel, Alvina Hoffmann, Oliver Kearns, and Sebastian Larsson, 'Collective discussion: Toward critical approaches to intelligence as a social phenomenon', *International Political Sociology*, 14:3 (2020), pp. 323–344 (p. 325); Sophia Hoffman, Noura Chalati, and Ali Dogan, 'Rethinking intelligence prac- tices and processes: Three sociological concepts for the study of intelligence', *Intelligence and National Security*, 38:3 (2023), pp. 319–38.

[107]Neumann and Sending, 'Expertise and practice', pp. 30–1.

[108]Ibid., p. 36; Damien Van Puyvelde and Sonia Sangiovanni, 'Private sector intelligence', in Robert Dover, Huw Dylan, and Michael Goodman (eds), *A Research Agenda for Intelligence Studies and Government* (Cheltenham: Edward Elgar, 2021), pp. 103–11.

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

dominant OSINT narrative sideline other pressing global challenges like climate change and global health? Do alternative OSINT discourses exist beyond the Global North, and if so, how do they differ in their focus?

Third, the ethical and legal challenges posed by OSINT require further attention. Early con- tributions have explored the tension between the social good and potential harm caused by open-source investigations and digital activism.[114] This concern extends beyond government agen- cies,[115] to include private sector data brokers and consultancies whose practices often escape rigorous scrutiny,[116] as well as civil society groups and hobbyists. OSINT techniques can enable harmful practices like doxing – the intentional online publication of private information – raising serious ethical questions about their use. In one case, online sleuths were urged to use publicly avail- able data to track rioters who attended the 6 January 2021 attack on the US capitol, leading to the misidentification and public harassment of at least one individual.[117] Both government agencies[118] and investigative groups[119] are working to develop norms that guide their practices and mitigate potential harm. Scholars focused on the ethics of intelligence and security have an important role to play in developing standards for the responsible use of digital fieldwork and integrating these to the broader body of knowledge on social science research methods.[120] Ultimately, further research is needed to explore how OSINT can contribute responsibly to security studies and aid efforts to govern the increasingly complex information landscape that informs and defines much of the field.

[109]Simon Chesterman, 'We can't spy … if we can't buy!': The privatization of intelligence and the limits of outsourcing 'inherently governmental functions", *European Journal of International Law*, 19:5 (2008), pp. 1055–74; Damien Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability* (Edinburgh: Edinburgh University Press, 2019).

[110]For a similar point, see Lene Hansen, 'Theorizing the image for security studies: Visual securitization and the Muhammad cartoon crisis', *European Journal of International Relations*, 17:1 (2011), pp. 51–74.

[111]Haas, 'Epistemic communities and international policy coordination', p. 3; Judith Reppy, 'Producing knowledge for the military: Experts and amateurs in the national security community', in Trine Villumsen Berling and Christian Bueger (eds), *Security Expertise: Practice, Power, Responsibility* (London: Routledge, 2015), pp. 125–140 (p. 127); Vaibhava Shetty, 'The role of non-elites and eyewitness videos in the visual securitisation of Calais asylum seekers', *European Journal of International Security*, 7:4 (2022), pp. 413–434 (p. 420).

[112]Joseph Downing and Richard Dron, 'Theorising the "security influencer": Speaking security, terror and Muslims on social media during the Manchester bombings', *New Media & Society*, 24:5 (2022), pp. 1234–57.

[113]Private information, 2019.

[114]Ben Loehrke, Laura Rockwood, Melissa Hanham, and Lisa Kenausis, *The Gray Spectrum: Ethical Decision Making with Geospatial and Open Source Analysis* (Muscatine, IA: Stanley Center for Peace and Security, 2019); Hanman and Shin, *Ethics in the Age of OSINT Innocence*; Sebastián Galleguillos, 'Digilantism, discrimination, and punitive attitudes: A digital vigilantism model', *Crime, Media, Culture: an International Journal*, 18:3 (2021), pp. 353–74.

[115]Thorsten Wetzling and Kilian Vieth, 'Legal safeguards and oversight innovations for bulk surveillance: An international comparative analysis', in Lora Anne Viola and Pawel Laidler (eds), *Trust and Transparency in an Age of Surveillance* (London: Routledge, 2021), pp. 145–164.

[116]Urbano Reviglio, 'The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview', *Internet Policy Review*, 11:3 (2022), pp. 1–27; Arango, 'Data brokers'.

[117]Rachel Sherman, 'The dark side of open source intelligence', *Coda* (15 January 2021), available at {https://www.codastory. com/authoritarian-tech/negatives-open-source-intelligence/}.

[118]Department of Homeland Security, *Public–Private Analytic Exchange Program: Ethical Framework in Open-Source Intelligence* (2022), available at {https://www.dhs.gov/sites/default/files/2022-09/Ethical%20Frameworks%20in%20OSINT%20Final.pdf}.

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

Acknowledgements. The authors would like to thank participants in the workshop they organised on 'OSINT and the war in Ukraine', University of Leiden, 2024. The lead author used an AI agent he trained to assist with copyediting the initial article manuscript, focusing on clarity and grammar.

Funding statement. Research for this paper is part of a project entitled 'Open-source research and the war in Ukraine: Intelligence for the people by the people?' (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).

Damien Van Puyvelde is Associate Professor and Head of the Intelligence and Security Research Group at Leiden University.

Fernando Tabarez Rienzi is Open Source Investigator at the Centre for Information Resilience.