Stanley Center
FOR PEACE AND SECURITY

ANALYSIS & NEW INSIGHTS

Public Open Source Analysis and Intelligence

Practice, Terminology, and Ethical Considerations

By Neil Ashdown | October 2022

Abstract

Open source intelligence (OSINT) analysis is an established discipline within the US and UK national security intelligence communities. However, the term is also regularly applied to the activities of a heterogenous ecosystem of actors in the public sphere. This paper examines the ethical implications of the use of the same term to refer to these different activities. It draws out ethically relevant differences between government intelligence practices and the practices of public open source analysts. These differences often center on the lack of accountability around public open source analysis. This paper argues for greater rigor in the use of the term "intelligence" as part of a broader effort to articulate the values and objectives of public open source analysis.

Introduction

Media coverage of the war in Ukraine has drawn on multiple sources of information. One important stream has been the public disclosure of intelligence by Western governments.[1] However, these official disclosures have been accompanied by a wealth of analysis conducted by people outside government, working with open sources such as social media and commercial satellite imagery. The ability of these public open source analysts to track equipment losses and map the ebb and flow of fighting has itself become part of the wider story of the invasion.[i]

1 See, for example, the regular updates provided by UK Ministry of Defence on Twitter, including, "Latest Defence Intelligence Update on the Situation in Ukraine—11 July 2022," accessed July 14, 2022, https://web.archive.org/web/20220712121613/https://twitter.com/DefenceHQ/status/1546361867320365058.

This focus has added to the already high interest surrounding public open source analysis[2] of international security and proliferation issues, ranging from the downing of civilian airliners to developments in North Korea's nuclear program to the expansion of China's ballistic missile program.[ii] Part of the popular interest in this subject arises from the perception that people working outside government can now use open sources of information to duplicate capabilities that have historically been restricted to governments.[3]

A wide range of people and organizations use information available in open sources to produce intelligence. Open source analysts work in government, in the private sector, in civil society organizations, and among the public. Complicating the picture, these individuals often move back and forth between roles over time. For example, an analyst may learn their trade in government or a large, private sector intelligence provider before starting their own consultancy, or going to work for a civil society organization, or simply publishing open source analysis on social media in their spare time.

Crucially, although these roles all involve open source information, the practices involved will differ between governments, the private sector, and the public. The experiences and activities of an analyst working with open source material in a government agency will differ from those of a member of the public working with open sources and publishing analysis on social media. This is the case even when public analysts use capabilities such as satellite imagery that were once restricted to governments, and conversely when government agencies conduct analysis using open sources. This paper does not argue that one of these activities is more important or ethical than another. Instead, it examines the differences between these practices and highlights ethically relevant considerations.

In addition, this paper argues that some activities described as open source intelligence are not intelligence in a meaningful sense.[4] Again, this does not mean these activities are unethical or less valuable. However, this paper does consider some risks inherent in applying the term "intelligence" to activities that are better understood as other forms of knowledge production, such as journalism, and it argues for practitioners to reflect on the characterization of their work. Such critical reflection is an integral part of wider efforts to promote ethical decision making in open source analysis.[5]

Comparing Government OSINT and Public Open Source Analysis

Government intelligence capabilities can provide unparalleled insights into matters of critical importance, using sources and methods that cannot be duplicated by members of the public. Nonetheless, it would be a mistake to infer from these descriptions that public open source analysis offers only a limited approximation of state intelligence capabilities.

Public open source analysis can bring together diverse and unlikely sources of information, analyze them using novel and experimental methodologies, and make the outcomes of these processes widely and rapidly available to inform, invite comment, and challenge orthodoxies. Investigations and research conducted in open sources can be agile, socially inclusive, crosscutting, and innovative in a way that governments and militaries, operating under security restrictions and with pressing missions, struggle to duplicate.

As a simplified characterization, government intelligence activity is conducted by officials, military personnel, and vetted contractors, in secure facilities under security restrictions. A depth and scale of analytical resource and experience can be brought to bear that is unlikely to be duplicated outside of the agencies. Intelligence products are disseminated in a controlled fashion to intended users or else feed into other intelligence functions as intermediate outputs. Intelligence will be produced against an operational requirement and is intended to guide action.

By contrast, it is challenging to identify a single model of public open source analysis as a social practice, even as a simplification. To see this, note that the term "OSINT analysis" as commonly used could be applied to:

- A person analyzing imagery from Google Earth alone in their bedroom after work and publishing that material on Twitter.
- A team of academics, journalists, and former military satellite imagery analysts, working in transnational partnership with commercial satellite imagery providers and government-funded think tanks, to publish reports that receive international media coverage.

2 The term "public open source analysis" admittedly risks confusion given the use of the word "public" to refer to government, as in "public sector." However, the term "nongovernmental open source analysis" is less concise and does not imply the act of publication.

3 See, for example, the claim that "[w]hat was then world-historic is now the stuff of student projects" in "Open Source Intelligence Challenges State Monopolies on Information," *Economist*, August 7, 2021, https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information.

4 This paper is not a return to the debate about whether open source intelligence counts as "real" intelligence, or whether that status only applies to secret intelligence. I argue that it is entirely possible for an organization or individual operating outside government using only open sources to conduct intelligence activity.

5 The Stanley Center for Peace and Security has promoted practical discussions around ethical decision making in open source analysis through a series of workshops and reports.

As these examples suggest, public open source analysis can be conducted by heterogenous networks of actors. For some people, this work will be a hobby rather than their profession. Open source investigations and analysis rely on a different combination of sources than government intelligence activity; some sources will overlap with those available to states (such as satellite imagery) and others (such as social media) may be *less* accessible to government officials because of domestic regulatory regimes or the classification of intelligence requirements. Processes for verifying and analyzing information will vary dramatically among public open source analysts, with the majority likely adopting less-stringent processes than are used within government. Reporting will often be published online, making it theoretically accessible to billions of people. Moreover, this work is unlikely to address a direct operational requirement, even if the information produced may be of use to a decision maker.

Caveat on the Depictions of Government Intelligence Practices

This paper's depiction of intelligence practice within government agencies is based on accounts from journalists and former practitioners, along with the academic literature on intelligence. As such, it comes with the caveat that there may be aspects of government intelligence practice that are not reflected in publicly available information; this could apply as much to methods of analysis as to technical collection. This account is also focused primarily on single-source collection and all-source intelligence assessment processes in the US and UK intelligence communities. The actual day-to-day practices of intelligence agencies in many parts of the world vary considerably.

Systems of Accountability

Systems for accountability represent a key difference between government intelligence activity and public open source analysis. In Western liberal societies, intelligence agencies are intended to be accountable to democratically elected representatives. Former UK intelligence official Sir David Omand refers to a social compact between the people and their representatives, on the one hand, and the state and its agencies on the other hand.[iii] This compact provides the agencies with a "social license" to operate in secret and to conduct under warrant activities that would otherwise be illegal.

An action may be legal and still be unethical. Hence, Omand and intelligence studies academic Mark Phythian note that to be ethical, intelligence activity must be "in accordance with the constraints of statute law, transparent to the public, and with the intended meaning of terms such as 'national security' explained in published government documents."[iv]

There have certainly been instances when these systems of accountability and oversight have not functioned correctly. What is key here is that whatever weaknesses such systems may have, there are no similar systems governing the work of public open source intelligence analysts. Analysts outside government, including in most of the private sector,[6] are not accountable to democratic representatives, do not have the same legal protections for their work, and cannot claim national interest justifications for their actions in the same way as state actors.

With government intelligence analysis, the activity of intelligence is secret. However, there are defined lines of accountability, centralized standards, and enforcement mechanisms. With public open source analysis, the situation is reversed. The activity is (largely) transparent. However, it is not clear to whom practitioners are accountable, by what standards, and with what enforcement mechanisms. With government intelligence activity, the process is secret, but the identity of the end user is clear; it is the state. With public open source analysis, the process is conducted in the open, but it is unclear who uses the information or for what purpose.[v]

Tasking and Collection Methods

The intelligence collection activities of government agencies—from open source research through to human or technical intelligence—are intended to be conducted in line with national interests. In contrast, public open source analysts are largely self-tasking. The motivations behind an analyst's choice of subject matter range widely, from personal interest in the topic to advancing a political or ideological agenda to financial gain.[7]

There have been calls for open source practitioners to be more explicit about these motivations—in effect, to explain how they "task" themselves. For example, cybersecurity researchers Ronald Deibert and Masashi Crete-Nishihata describe how they use "research warrants" that "outline the nature and justification for all aspects of the research, which are then incorporated into the text of the published reports."[vi] These documents have no special legal status, and they certainly do not provide a national security justification for these investigations. However, there is value for the researchers and for external observers in the creation of a document that makes the practitioners' rationale for their work explicit.

The national security justification of state intelligence activity also theoretically justifies the use of intrusive collection methods by state agencies. Secret intelligence collection is inherently adversarial—it is about stealing secrets—and therefore raises stark ethical questions.[vii] In contrast, public open source analysts

6 Companies providing in-house intelligence services to government agencies under contract arguably fall within the scope of the state for the purposes of this discussion, albeit with legal and ethical differences.

7 This motivation is not limited to the private sector—the proliferation of platforms for monetizing social media content is likely to be having a substantial impact on the development of the public open source analysis space.

cannot appeal to reasons of state or national security and hence cannot justify intrusive, adversarial collection methods.

Rather, in the public open source space, the key debate is over what constitutes "open source." Establishing policies and guidelines for these decisions requires ethical reflection. This is an ongoing process, since the set of information that is considered open source changes over time and will differ between individuals and organizations. For example, social media investigations can require researchers to circumvent platform restrictions on access through technical means or through deceptive activities such as the creation of false personas. This moves social media investigations closer to online human intelligence, an activity that in many jurisdictions will be restricted by law to properly mandated government agencies. Even when information on social media platforms is entirely open, there remains the need for an awareness of ethical risks. The inclusion of information in published analysis could bring negative consequences for the originator of that information.[8] The originator of information on social media may not be aware of that information's analytic value, complicating decisions around the reuse of the information even if the originator has no reasonable expectation of privacy around the information.

Resources and capability will also shape what sources are "open" to an analyst or organization. Google Earth is available to anyone with an internet connection. However, more-sophisticated open source analysis generally requires access to high cadence or more up-to-date imagery or to specialized forms of imagery, such as synthetic aperture radar. While this imagery is technically available to any member of the public, it requires specialized skills to analyze, its price may be prohibitive, and in practice, access may depend on social connections and the release policy or competitive taskings of the imagery provider.

Organizations will also differ in their risk appetites around sources. For example, leaked data can be purchased via social media platforms or on the dark web for a nominal fee. Some civil society organizations consider this to be open source while others are prohibited by internal policies from using such material. Neither position is straightforwardly correct, highlighting once again the importance of critical reflection and debate on these issues among public open source analysts.

Ethical Research in Cybersecurity

Cybersecurity researchers are another group of practitioners seeking to determine how their research relates to existing practices of knowledge production. A 2011 article by Deibert and Crete-Nishihata described a closed-door workshop intended to further "an ethical, normative, and legal framework" to guide cybersecurity research.[viii] Part of the impetus behind that workshop was the authors' belief that academic research ethics frameworks were ill-suited to cybersecurity research. Similarly, David Dittrich et al. outlined longstanding challenges to ethical research in information security, raising many of the same issues that have been highlighted by open source analysts.[ix] These included concerns over research being driven by the news agenda, about responsible disclosure of information of value to adversaries, and about the perceived lack of shared community values.

The Ethics of Analysis

The quality of analysis is relevant to its ethical character. This connection is especially clear when governments work with the kind of intelligence that is likely to be directly relevant to military or law enforcement operations. As Omand and Phythian note, "The intelligence analysts have a responsibility to behave ethically in the way they infer rational conclusions from intelligence material and in the confidence they ascribe to those judgements, for their conclusions may well have serious, even fatal consequences for those individuals against whom action is subsequently taken."[x] In contrast, while public open source analysis can still cause harm, this will usually be an undesirable side effect.[xi]

This prompts empirical questions about the quality of analysis conducted by public open source analysts, as well as normative questions around the standards by which the quality of analysis is assessed. Answering the empirical question is beyond the scope of this paper. However, two preliminary observations can be offered.

First, no organization has a monopoly on good analysis. For most of the 20th century, the direction of travel was for methodologies for intelligence analysis and data processing developed in government and the military to move into the public sphere. Increasingly, however, it is governments that are turning to external actors for cutting-edge data processing and analysis capabilities.[xii] The impact of advances in behavioral and cognitive psychology on the development of intelligence analysis methodologies in the Western intelligence community from the 1970s onward could be seen as an earlier example of government analytic communities learning from external actors.[9]

Second, it is likely that the quality of analysis varies widely among public open source analysts. Despite the adoption of the trappings of structured analytical techniques among public open source analysts and private intelligence providers, it is an open

8 For discussion of these and other ethical issues, see Benjamin Loehrke, Luisa Kenausis, Aida al-Kaisy, Devon Terrill, and Kelly Smits, *Feeling the Burden: Ethical Challenges and Practices in Open Source Analysis and Journalism*, Stanley Center for Peace and Security, January 19, 2022, https://stanleycenter.org/publications/ethics-osint-analysis-journalism/.

9 The canonical example would be Richards J. Heuer, *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, US Central Intelligence Agency, January 1, 1999, https://apps.dtic.mil/sti/citations/ADA500078.

question how effectively these processes are applied.[10] There is a fundamental difference between, on the one hand, approaches that aim to assemble all the available information into a coherent mosaic and, on the other hand, approaches that assess each piece of information independently before composing an overall assessment.[xiii] The latter is good intelligence analysis, but the former can produce compelling narratives. Depending on the motivation behind the publication of the material, the latter may be a decisive consideration.

Processes for imposing standards for analysis can be established within hierarchical organizations—such as government agencies—as a condition of membership. However, attempting to impose similar authorities on what can be construed as matters of opinion or expert judgement within the public sphere is fraught with difficulties around rights to freedom of expression and thought. A recurring theme in discussions among open source practitioners organized by the Stanley Center for Peace and Security is that the creation of a central clearinghouse to act as an authority on open source analysis presents considerable challenges. Participants in these discussions note that in practice, standards for analysis among the public open source community are determined intersubjectively, with no recourse for enforcement against individuals and organizations that do not subscribe to proposed standards.

Open Source Analysis and Vicarious Trauma

The open source community is increasingly aware of the risks involved in the practice of analyzing disturbing material. For analysts examining ongoing conflicts, human rights violations, or criminal activity, their work can involve prolonged periods of intense examination of disturbing material. There is a growing recognition that this exposure can have psychological impacts on the analysts. This phenomenon is variously termed vicarious trauma or witness-related trauma. Emerging understanding of vicarious trauma is based largely on anecdotal accounts from within the community. This is an area where further interdisciplinary research is urgently required. If the practice of open source analysis on certain topics carries foreseeable risks of psychological harms to the practitioner or to people exposed to reporting—as seems credible—then this is relevant to the ethical character of the activity.

The Ethics of Publication and Dissemination

The biggest difference between government intelligence activity and public open source analysis is how the products of these practices are disseminated. In government intelligence activity, the goal is for the intended user to receive the intelligence product uniquely via controlled systems within a timescale and in a format that makes it actionable.

Beyond this basic function, intelligence might be disseminated more broadly or made public for reasons ranging from intelligence alliances and liaison arrangements to combating disinformation. These decisions will inevitably also have an ethical component. Virtually any disclosure of declassified intelligence, by potentially enabling inferences about sources and methods—or simply by increasing an adversary's awareness—has the potential to reduce the effectiveness of future intelligence collection. Decision-making processes, therefore, need to consider the possibility of a disclosure now leading to a future intelligence failure, with all the possible ethical ramifications of such a scenario.

The picture is very different when analysis is published online. Indeed, where analysis is produced through open discussions and online crowdsourcing, that analysis is being continually published throughout its production, preempting any decisions around the release of the final product.

Once public open source analysts publish information, they lose virtually all control over its use and distribution. This is a crucial point and highlights a key area for ethical reflection among public open source practitioners. Government agencies strictly control the dissemination of intelligence to ensure it is used only by its intended recipients. Conversely, once material is published, a practitioner has no control over how the material is used or by whom. This applies not just to the content of the analysis but also to the methods used in its production, which may be explicit or discernible in the product itself. If this information is used by other actors in ways that are unethical, the originating analyst may be ethically culpable.

Similarly, public open source analysts also need to consider source-protection issues. Some open sources are effective precisely because—while public—they are little known. For example, publicly accessible webcams providing useful views of military facilities and ports have been disconnected after their existence was highlighted in published reporting. These changes reduce the potential future value of these sources for all analysts, which may have ethical consequences.

The pace of dissemination is also different between government and public open source analysis. The decision to publicly disclose declassified intelligence produced by state agencies is a protracted one. US disclosures of declassified intelligence around Russia's invasion of Ukraine in 2022 came amid growing pressure from both former and serving national security officials to sanitize and more widely release declassified intelligence.[xiv] In contrast, analysts working outside government can and do publish their work with a single click. Some higher profile or better resourced public open source analysis organizations have formal processes for approving the release of their reporting, often implicitly or

10 See, for example, the analysis of the varying quality of commercial cyberthreat intelligence offerings in J. D. Work, "Evaluating Commercial Cyber Intelligence Activity," *International Journal of Intelligence and CounterIntelligence* 33, no. 2 (2020): 278–308.

explicitly parallelling the editorial processes used by journalistic organizations. However, many public open source analysts will make decisions about publication independently and without processes for peer review prior to the release of the material. Challenge often comes once material is published, but subsequent changes to assessments consistently receive less attention than the original publication.

Finally, publication is suggestive of a very different intent than the controlled distribution of information to support the decisions of specific actors. The decision to publish may be driven by the analyst's view of the public interest, their desire to share information about a topic they are enthusiastic about, or to advance a political or ideological agenda. It may also be driven by the desire for attention, prestige, or commercial gain. It can certainly be ethical to publish material based on such motives, but they introduce problematic incentives that require critical reflection. For example, if the analyst's goal is to attract attention, then this introduces biases around the speed of publication and the conclusions drawn; an earlier, more sensational report will almost certainly receive greater attention than its more considered successor.

The Role of Intent in Defining Intelligence Activity

This question of intent goes to the heart of the distinction between intelligence and other forms of knowledge production. Definitions of intelligence that restrict it to the activities of government agencies are too narrow to account for the range of nonstate actors that conduct intelligence activity.[xv] Conversely, a definition of intelligence that expands to include any sensemaking activity is too broad to reflect common usage; there are meaningful distinctions between intelligence, journalism, and academic research, for example.

The working definition of intelligence used in this paper is, therefore, that intelligence is sensemaking activity that supports a decision maker. Such a definition is present in the academic literature.[11] It also aligns with the definition given in the *Berkeley Protocol on Digital Open Source Investigations*, where intelligence is defined as a subset of information "collected and used for the specific purpose of aiding policymaking and decision-making, most often in a military or political context."[xvi]

This definition means that the key to determining whether a particular activity or product is intelligence is the intent underlying the activity.[12] The difference between a well-researched piece of investigative journalism and an intelligence report is not so much in the content of either artifact but in the reason for its production. If the material was produced with the intent to support a decision maker, then that activity was intelligence; if it was to inform the public, it was journalism.

This definition distinguishes intelligence from other activities conducted by intelligence agencies, such as covert action.[13] Moreover, it would include some—but by no means all—of the activities that are often branded "open source intelligence" in the media and by practitioners. Where public open source analysts are engaged in a sensemaking process intended to support a decision maker, that activity would be open source intelligence. However, using this definition, much public open source analysis would be better understood as journalism, scholarship, or other activities such as marketing or public relations.[14]

Ethical Implications of Using the Term "Intelligence"

The term "intelligence" might be applied to activities that are not intelligence related for several reasons. The first is simple confusion about the nature of the activity. Although not malicious, this is nonetheless suggestive of a lack of reflection on the activity in question—in turn suggesting a possible lack of reflection around the ethical challenges associated with this activity. The use of the term "intelligence" may also reflect deliberate exaggeration; there is an undeniable cachet around intelligence, and this is reflected in its use in commercial marketing materials or for attracting attention on social media. The term may even be used deceptively, exploiting the supposed credibility of open source analysis to spread disinformation.[xvii]

Using the term "intelligence" also introduces a range of practical issues. As noted above, it may lead to observers viewing the activity in a positive light, as more credible or interesting. However, the term can also attract negative attention. In many parts of the world, the perception that a person is conducting intelligence activities can attract the attention of the authorities, with potentially harmful consequences. Labeling public open source analysts as "citizen spies" or "Twitter spies" inaccurately conflates intelligence with espionage and creates the risk of harm.[xviii] This suggests that even when the use of the term "intelligence" is accurate, there might be practical and ethical reasons to use other terms.

11 See, for example, the discussion of the characteristics of intelligence in Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem," *Intelligence and National Security* 36, no. 2 (October 30,2020), http://www.tandfonline.com/doi/abs/10.1080/02684527.2020.1840746; or of intelligence theory versus empirical investigation in Mark Stout and Michael Warner, "Intelligence Is as Intelligence Does," *Intelligence and National Security* 33, no. 4 (June 7, 2018): 517–26, https://doi.org/10.1080/02684527.2018.1452593.

12 This point was made independently by two former government intelligence practitioners in discussions around this paper.

13 For a discussion of this point, see Stout and Warner, "Intelligence Is as Intelligence Does."

14 "A meaningful subset of what is disseminated as cyber intelligence reporting originating from vendor entities must also be considered merely as marketing collateral." Work, "Evaluating Commercial Cyber Intelligence Activity," 292–93.

Public open source analysts should, therefore, reflect on whether the activity they are conducting really is intelligence. If it is not, then for all the reasons set out above, a more appropriate term should be used. Significantly, Bellingcat—one of the organizations most associated with the term "open source intelligence"—does not use the term to describe its own activities. Instead Bellingcat describes itself as "an independent international collective of researchers, investigators and citizen journalists using open source and social media investigation to probe a variety of subjects."[xix] Its "Editorial Standards & Practices" document includes the word "intelligence" only once ("information from an anonymous source should only be used as an *intelligence* lead" [emphasis added]), while making clear that the organization is committed to journalistic and research ethics.[xx]

Disrupting Communities of Practice in Knowledge Production

As academics Florian Egloff and Myriam Dunn Cavelty argue, "Our ways of pursuing knowledge are never neutral but subjective and embedded in a historically grown system of practices that tell us 'how to do things the right way.'"[xxi] Roles such as journalist, lawyer, or intelligence analyst are socially constructed and prone to change over time. These practitioners are to varying extents expected to engage in ethical deliberation to guide these decisions, usually as part of a community of practice.

Moreover, a person's claim to be acting within one of these frameworks is partly a performance, the success of which depends on its acceptance by the intended audience. The determination of who is a journalist, for example, is intersubjective; it is partly about calling yourself a journalist, but that description must also be accepted by other people. The same is true of being an academic or an intelligence analyst.

Over time these performances become increasingly entrenched, to the point where they can come to be taken for granted. Some become heavily formalized around a single membership and system of authority, as with lawyers and medical practitioners. Others are less formalized but nonetheless recognized as communities with standards of practice, such as journalism. Nonetheless, all these roles remain constructed and intersubjective, and hence open to incremental change as well as disruption.

Current understandings of what it is to be an intelligence analyst—and indeed the term "OSINT" itself—are a legacy of a historical period where intelligence activity was concentrated in government agencies.[xxii] In historical terms, this period is relatively recent—there is a long history of intelligence activity preceding the creation of formalized state intelligence agencies or the modern state.[xxiii] The concentration of intelligence activities in state agencies peaked in the second half of the 20th century, when the nuclear standoff of the Cold War placed an overwhelming premium on information that could be generated through state capabilities.[xxiv]

Heading into the 21st century, the privatization of many state functions, the private sector's growing dominance in technological development, and the rise of complex transnational threats are once again shifting the constellation of actors engaged in intelligence work. These dynamics have disrupted understandings of what it is to practice intelligence. The open source analysis of satellite imagery is the iconic example of this dynamic; earth observation satellites were a technology developed by and for government intelligence apparatuses that over time entered the commercial sphere and began to be used by people outside government.[xxv] The role of social media in allowing people to access granular information from areas of interest in near real time, and to easily publish their findings, has been even more transformative. Amid this transformation, it is unsurprising that roles such as journalist and intelligence analyst are being disrupted.

Conclusion

It is now possible, because of technological changes, for an individual outside government to access information that previously was restricted to state agencies, such as satellite imagery, or which previously took considerable resources to access, such as contemporaneous reporting from around the world. Individuals can use these capabilities to produce reporting that in many ways approximates the outputs of government intelligence functions. This capability has given a new set of actors a voice in public discussions about international security.

This transformation has brought a wide range of benefits. However, it has also outpaced intersubjective understandings of different roles in knowledge production, with the result that the status of this activity within societies remains contested. This can be seen in confusion over the application of the term "intelligence." It can also be seen in the lack of consensus over issues of accountability and the application of ethical standards for collection, analysis, and publication among open source analysts.

Understandings of the nature of public open source analysis will be shaped primarily by the daily practices of the community—something that should prompt reflection among practitioners. Public open source analysis from reputable outlets currently enjoys a high degree of credibility with the public in developed Western states.[xxvi] The maintenance of this credibility requires a commitment to high-quality, responsible analysis.

However, these understandings will also be shaped by deliberate public interventions. Examples include Bellingcat's description of its own activities referenced above, the Open Nuclear Network's publicization of its *Code of Ethics* in June 2020,[xxvii] the release of the *Berkeley Protocol* in January 2022,[xxviii] or the ongoing work of the Stanley Center on promoting ethical decisionmaking in open source analysis. Both in their daily practice and in these public interventions, practitioners are engaged in a performance intended to encourage others to accept their claims to expertise.

The acceptance of this performance will depend on a wide range of factors. However, individuals and analysts are more likely to be successful if they can, first, clearly outline the nature of their activity and, second, show they are committed to standards of good and ethical practice. The first task requires a rigorous consideration of the applicability of the term "intelligence" to the activities being described. The second is less about demonstrating a perfect record of ethical decision making and more about emphasizing the standards to which practitioners are willing to be held and the processes they use to make these decisions.

These efforts are unlikely in the foreseeable future to lead to the creation of a single authority to formalize the practice of public open source analysis. However, they may contribute to the creation of a plurality of increasingly widely recognized communities of practice with broadly shared goals and values, committed to making the case for the value of open source analysis to the public.

Recommendations

The following three recommendations for practitioners working in this space are focused on critical reflection and making explicit considerations that are often left unstated. Practitioners who have not reflected on these decisions may struggle to explain them to external observers at a time when open source analysis is coming under ever greater public scrutiny.

- **Practitioners should reflect on the terminology they use to describe their work.** Characterizing activity as "intelligence" has practical and ethical implications. Where public open source analysts are engaged in intelligence activity they should reflect on the differences between their work and government intelligence activity. Where these analysts are not engaged in intelligence activity, other, more appropriate terms should be adopted.

- **Critical reflection could be encouraged through the process of documenting individual or organizational practices and decisions.** Producing a written statement of a practitioner's general principles and specific research warrants for individual projects serves to encourage the process of reflection and make explicit to outside observers the goals and rationale of a project. Over time, these writings could contribute to a body of material documenting past decisions and practices in this field.

- **Practitioners could build on these reflections by publicly promulgating standards and good practices for their work.** Such standards should go beyond questions of ethical collection activities and the accuracy of analysis, encompassing the processes by which practitioners decide which subjects to work on and how the product of their analysis is shared, including around decisions about what to publish and when.

Endnotes

i Matt Freear, "OSINT in an Age of Disinformation Warfare," March 14, 2022, accessed March 15, 2022, https://rusi.org/explore-our-research/publications/commentary/osint-age-disinformation-warfare; Alison Bath, "Open Source Intelligence Observers Gain Growing Role in How War Is Viewed," *Stars and Stripes*, March 29, 2022, accessed 7 April 2022, https://www.stripes.com/theaters/europe/2022-03-29/citizen-osint-analysts-chronicle-russian-navy-role-in-war-in-ukraine-5513788.html.

ii Chris Stokel-Walker, "How Digital Sleuths Unravelled the Mystery of Iran's Plane Crash," *Wired UK*, January 13, 2020, accessed April 12, 2022, https://www.wired.co.uk/article/iran-plane-crash-news; Melissa Hanham, *Using Open Source Intelligence to Verify a Future Agreement with North Korea—New Approaches to Verifying and Monitoring North Korea's Nuclear Arsenal*, Carnegie Endowment for International Peace, July 27, 2021, accessed April 12, 2022, https://carnegieendowment.org/2021/07/27/using-open-source-intelligence-to-verify-future-agreement-with-north-korea-pub-85006; Joby Warrick, "China Is Building More than 100 New Missile Silos in Its Western Desert, Analysts Say," *Washington Post*, June 30, 2021, accessed February 10, 2022, https://www.washingtonpost.com/national-security/china-nuclear-missile-silos/2021/06/30/0fa8debc-d9c2-11eb-bb9e-70fda8c37057_story.html.

iii David Omand, *Securing the State* (Oxford: Oxford University Press, 2014); David Omand and Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence* (Oxford: Oxford University Press, 2018).

iv Omand and Phythian, *Principled Spying*, 78.

v Amy Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton, NJ.: Princeton University Press, 2022), 232-234.

vi Ronald Deibert and Masashi Crete-Nishihata, "Blurred Boundaries: Probing the Ethics of Cyberspace Research," *Review of Policy Research* 28, no. 5 (2011): 536, https://doi.org/10.1111/j.1541-1338.2011.00521.x.

vii Omand and Phythian, *Principled Spying*.

viii Deibert and Crete-Nishihata, "Blurred Boundaries."

ix David Dittrich, Michael Bailey, and Sven Dietrich, "Building an Active Computer Security Ethics Community," *IEEE Security Privacy* 9, no. 4 (2010): 32–40, https://doi.org/10.1109/MSP.2010.199.

x Omand and Phythian, *Principled Spying*, 227.

xi Loehrke et al., *Feeling the Burden*.

xii Neil Ashdown, "Connecting the Dots: Data Sense-Making Rises as National Security Requirement," *Jane's Intelligence Review*, July 8, 2021; Neil Ashdown, "Sensemaking, Systemic Competition, and the Social Compact," in *Futures Student Essay Competition* (Defence Science and Technology Laboratory, November 2021), 38–46, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1042677/Journal_FINAL_Student_Comp.pdf.

xiii Amy Zegart, *Spies Like Us*, 168-173, 237.

xiv Gordon Corera, "Ukraine: Inside the Spies' Attempts to Stop the War," *BBC News*, April 9, 2022, Europe, https://www.bbc.com/news/world-europe-61044063.

xv Michael Warner, "Wanted: A Definition of 'Intelligence,'" Studies *in Intelligence* 46, no. 3 (2002): 15–22. Warner has advanced alternative definitions of intelligence in his later work.

xvi *Berkeley Protocol on Digital Open Source Investigations*, Human Rights Center, University of California Berkeley, accessed July 14, 2022, https://humanrights.berkeley.edu/berkeley-protocol-digital-open-source-investigations.

xvii Chris Stokel-Walker, "Russia Co-Opts Grassroots Intelligence to Spread Propaganda," *New Statesman* (blog), March 18, 2022, https://www.newstatesman.com/internet-social-media/2022/03/russia-co-opts-grassroots-intelligence-to-spread-propaganda.

xviii Evan Ramstad, "Gulags, Nukes and a Water Slide: Citizen Spies Lift North Korea's Veil," *Wall Street Journal*, May 22, 2009, accessed April 12, 2022, https://www.wsj.com/articles/SB124295017403345489; Pranshu Verma, "The Rise of the Twitter Spies," *Washington Post*, March 23, 2022, accessed April 11, 2022, https://www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence-ukraine/.

xix Bellingcat, "About," accessed April 11, 2022, https://www.bellingcat.com/about/.

xx Bellingcat, "Editorial Standards & Practices," accessed April 11, 2022, https://www.bellingcat.com/app/uploads/2020/09/Editorial-Standards-Practices.pdf.

xxi Florian J. Egloff and Myriam Dunn Cavelty, "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics," *Journal of Cybersecurity* 7, no. 1 (February 16, 2021): 3, https://doi.org/10.1093/cybsec/tyab002.

xxii Bowman H. Miller, "Open Source Intelligence (OSINT): An Oxymoron?," *International Journal of Intelligence and CounterIntelligence* 31, no. 4 (October 2, 2018): 702–19, https://doi.org/10.1080/08850607.2018.1492826.

xxiii Christopher Andrew, *The Secret World: A History of Intelligence* (London: Penguin, 2018).

xxiv Andrew Rathmell, 'Towards Postmodern Intelligence," *Intelligence and National Security* 17, no. 3 (September 2002): 87–104, https://doi.org/10.1080/02684520412331306560.

xxv Luc Frieden, "Newsgathering by Satellites: A New Challenge to International and National Law at the Dawn of the Twenty-First Century," *Stanford Journal of International Law* 25, no. 1 (1988-1989): 103–93; David E. Sanger and William J. Broad, "Tiny Satellites from Silicon Valley May Help Track North Korea Missiles," *New York Times*, July 6, 2017, World, https://www.nytimes.com/2017/07/06/world/asia/pentagon-spy-satellites-north-korea-missiles.html.

xxvi "Open Source Intelligence Challenges State Monopolies on Information," *Economist*.

xxvii *Code of Ethics*, Open Nuclear Network, June 25, 2020, accessed July 14, 2022, https://opennuclear.org/code-ethics.

xxviii *Berkeley Protocol*.

Bibliography

Andrew, Christopher. *The Secret World: A History of Intelligence*. London: Penguin, 2018.

Ashdown, Neil. "Connecting the Dots: Data Sense-Making Rises as National Security Requirement." *Jane's Intelligence Review*, July 8, 2021.

———. "Sensemaking, Systemic Competition, and the Social Compact." In *Futures Student Essay Competition*, 38–46. Defence Science and Technology Laboratory, November 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1042677/Journal_FINAL_Student_Comp.pdf.

Bath, Alison. "Open Source Intelligence Observers Gain Growing Role in How War Is Viewed." *Stars and Stripes*, March 29, 2022. Accessed April 7, 2022. https://www.stripes.com/theaters/europe/2022-03-29/citizen-osint-analysts-chronicle-russian-navy-role-in-war-in-ukraine-5513788.html.

Bellingcat. "About." Accessed April 11, 2022. https://www.bellingcat.com/about/.

———. "Editorial Standards & Practices." Accessed April 11, 2022. https://www.bellingcat.com/app/uploads/2020/09/Editorial-Standards-Practices.pdf.

Berkeley Protocol on Digital Open Source Investigations. Human Rights Center, University of California Berkeley. Accessed July 14, 2022. https://humanrights.berkeley.edu/berkeley-protocol-digital-open-source-investigations.

Code of Ethics. Open Nuclear Network. June 25, 2020. Accessed July 14, 2022. https://opennuclear.org/code-ethics.

Corera, Gordon. "Ukraine: Inside the Spies' Attempts to Stop the War." *BBC News*, April 9, 2022, Europe. https://www.bbc.com/news/world-europe-61044063.

Deibert, Ronald, and Masashi Crete-Nishihata. "Blurred Boundaries: Probing the Ethics of Cyberspace Research." *Review of Policy Research* 28, no. 5 (2011): 531–37. https://doi.org/10.1111/j.1541-1338.2011.00521.x.

Dittrich, David, Michael Bailey, and Sven Dietrich. "Building an Active Computer Security Ethics Community." *IEEE Security Privacy* 9, no. 4 (2010): 32–40. https://doi.org/10.1109/MSP.2010.199.

Egloff, Florian J., and Myriam Dunn Cavelty. "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics." *Journal of Cybersecurity* 7, no. 1 (February 16, 2021): tyab002. https://doi.org/10.1093/cybsec/tyab002.

Freear, Matt. "OSINT in an Age of Disinformation Warfare." Royal United Services Institute. March 14, 2022. Accessed March 15, 2022. https://rusi.org/explore-our-research/publications/commentary/osint-age-disinformation-warfare.

Frieden, Luc. "Newsgathering by Satellites: A New Challenge to International and National Law at the Dawn of the Twenty-First Century." *Stanford Journal of International Law* 25, no. 1 (1988-1989): 103–93.

Hanham, Melissa. *Using Open-Source Intelligence to Verify a Future Agreement with North Korea—New Approaches to Verifying and Monitoring North Korea's Nuclear Arsenal*. Carnegie Endowment for International Peace. July 27, 2021. Accessed April 12, 2022. https://carnegieendowment.org/2021/07/27/using-open-source-intelligence-to-verify-future-agreement-with-north-korea-pub-85006.

Heuer, Richards J. *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, US Central Intelligence Agency. January 1, 1999. https://apps.dtic.mil/sti/citations/ADA500078.

"Latest Defence Intelligence Update on the Situation in Ukraine—11 July 2022." UK Ministry of Defence on Twitter. Accessed July 14, 2022. https://web.archive.org/web/20220712121613/https://twitter.com/DefenceHQ/status/1546361867320365058.

Lindsay, Jon R. "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem" *Intelligence and National Security* 36, no. 2 (October 30, 2020): 260-278. http://www.tandfonline.com/doi/abs/10.1080/02684527.2020.1840746.

Loehrke, Benjamin, Luisa Kenausis, Aida al-Kaisy, Devon Terrill, and Kelly Smits. *Feeling the Burden: Ethical Challenges and Practices in Open Source Analysis and Journalism*. Stanley Center for Peace and Security. January 19, 2022. https://stanleycenter.org/publications/ethics-osint-analysis-journalism/.

Miller, Bowman H. "Open Source Intelligence (OSINT): An Oxymoron?" *International Journal of Intelligence and CounterIntelligence* 31, no. 4 (October 2, 2018): 702–19. https://doi.org/10.1080/08850607.2018.1492826.

Omand, David. *Securing the State*. Oxford: Oxford University Press, 2014.

Omand, David, and Mark Phythian. *Principled Spying: The Ethics of Secret Intelligence*. Oxford: Oxford University Press, 2018.

"Open Source Intelligence Challenges State Monopolies on Information." *Economist*, August 7, 2021. https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information.

Ramstad, Evan. "Gulags, Nukes and a Water Slide: Citizen Spies Lift North Korea's Veil." *Wall Street Journal*. May 22, 2009. Accessed April 12, 2022. https://www.wsj.com/articles/SB124295017403345489.

Rathmell, Andrew. "Towards Postmodern Intelligence." *Intelligence and National Security* 17, no. 3 (September 2002): 87–104. https://doi.org/10.1080/02684520412331306560.

Sanger, David E., and William J. Broad. "Tiny Satellites from Silicon Valley May Help Track North Korea Missiles." *New York Times*, July 6, 2017, World. https://www.nytimes.com/2017/07/06/world/asia/pentagon-spy-satellites-north-korea-missiles.html.

Stokel-Walker, Chris. "How Digital Sleuths Unravelled the Mystery of Iran's Plane Crash." *Wired UK*. January 13, 2020. Accessed April 12, 2022. https://www.wired.co.uk/article/iran-plane-crash-news.

———. "Russia Co-Opts Grassroots Intelligence to Spread Propaganda." *New Statesman* (blog), March 18, 2022. https://www.newstatesman.com/internet-social-media/2022/03/russia-co-opts-grassroots-intelligence-to-spread-propaganda.

Stout, Mark, and Michael Warner. "Intelligence Is as Intelligence Does." *Intelligence and National Security* 33, no. 4 (June 7, 2018): 517–26. https://doi.org/10.1080/02684527.2018.1452593.

Verma, Pranshu. "The Rise of the Twitter Spies." *Washington Post*. March 23, 2022. Accessed April 11, 2022. https://www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence-ukraine/.

Warner, Michael. "Wanted: A Definition of 'Intelligence.'" *Studies in Intelligence* 46, no. 3 (2002): 15–22.

Warrick, Joby. "China Is Building More than 100 New Missile Silos in Its Western Desert, Analysts Say." *Washington Post*. June 30, 2021. Accessed February 10, 2022. https://www.washingtonpost.com/national-security/china-nuclear-missile-silos/2021/06/30/0fa8debc-d9c2-11eb-bb9e-70fda8c37057_story.html.

Work, J. D. "Evaluating Commercial Cyber Intelligence Activity." *International Journal of Intelligence and CounterIntelligence* 33, no. 2 (2020): 278–308.

Zegart, Amy. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton, NJ.: Princeton University Press, 2022.

———. "Spies Like Us: The Promise and Peril of Crowdsourced Intelligence." *Foreign Affairs* 100, no. 4 (July/August 2021): 168-173.

About the Author

Neil Ashdown is a PhD candidate in the Centre for Doctoral Training in Cybersecurity at Royal Holloway University of London. His research examines the relationship between intelligence and cybersecurity. Prior to starting work on his PhD, Ashdown was an analyst and editor for UK defense intelligence company Jane's, most recently as the deputy editor of *Jane's Intelligence Review*.

About Us

The Stanley Center for Peace and Security partners with people, organizations, and the greater global community to drive policy progress in three issue areas—mitigating climate change, avoiding the use of nuclear weapons, and preventing mass violence and atrocities. The center was created in 1956 and maintains its independence while developing forums for diverse perspectives and ideas. To learn more about our recent publications and upcoming events, please visit stanleycenter.org.

This paper contains 100 percent post-consumer fiber, is manufactured using renewable energy—Biogas—and processed chlorine free. It is FSC®, Rainforest Alliance™, and Ancient Forest Friendly™ certified.

10/22