https://doi.org/10.1142/9781800614079_0010

Chapter 3.4

OSINT and the US Intelligence Community: Is the Past Prologue?

Kathleen M. Vogel

Abstract

This chapter will discuss the definition and history of open source intelligence (OSINT) within the US intelligence community, and the various cultural factors that have shaped its acceptance there. It reviews the US intelligence community's use of and attitudes to OSINT, and demonstrates that despite stating a commitment to OSINT, and setting up institutional arrangements for this, the sector has often been less enthusiastic about it than might be expected, with intelligence practitioners frequently preferring intelligence derived from classified sources. Finally, the chapter considers how the growth of digital technologies and publicly available information is putting pressure on the US intelligence community to change its working relationship with OSINT, and details ways in which it might do this.

Introduction

As the various chapters in this book reflect, there is a growing interest in and demand for open source information and open source intelligence (OSINT) to understand different national and international security concerns. There are also a variety of government and non-government entities that have entered the OSINT arena. In light of these developments, it is useful to ask the following question: What role does OSINT have and what role should it play within the US intelligence community (IC)?[1] This chapter looks at the historical development and use of OSINT within the IC, how cultural factors have shaped the incorporation of OSINT within intelligence practice, and how OSINT intersects with the growing information and communications revolution. It will also discuss particular challenges and opportunities OSINT poses to the IC now and in the future.

OSINT

At the outset, it is important to clarify the distinction between open source information in general and OSINT as used within US intelligence.

Definitions and use

The IC defines open source information (either in verbal, written or electronic form)[2] as that which can be obtained legally, for instance, from the internet, a human source or physical locations that US or allied forces have taken control of.[3,4] Open source information[5,6] can include, in electronic or non-electronic form, various categories, such as the following: (1) traditional media (e.g. foreign and domestic television, radio and print media); (2) information obtained via the internet which includes online publications, online reviews, blogs, discussion groups, citizen media and user-generated content (e.g. people taking pictures with their cell phones and posting them), YouTube, and social media and networking sites (e.g.

[1] The US intelligence community comprises numerous organizations and activities spanning national intelligence, military intelligence, civilian intelligence and more. See https://www.intelligence.gov/ for more information about it.

[2] Richelson J. T. Open Sources, Site Exploitation, and Foreign Materiel Acquisition, in Richelson J. T. (ed.), *The US Intelligence Community,* 7th ed. New York: Routledge. 2015. pp. 346–369.

[3] *ibid.*

[4] By contrast, see e.g. the US Congress in the 2006 Defense Authorization Act, which defines OSINT as, ‘intelligence that is produced from publicly available information collected, exploited, and disseminated in a timely manner to an appropriate audience’. See: 109th Congress, *Public Law* 109–163–6 January 2006, National defense authorization act for fiscal year 2006, Subtitle D — Intelligence-Related Matters, Sec. 931. Department of Defense Strategy for Open-Source Intelligence. Available from: https://www.congress.gov/109/plaws/publ163/PLAW-109publ163.pdf [Accessed 28 July 2023].

[5] Hulnick A. The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence? In: Johnson L. K. (ed.), *The Oxford Handbook of National Security Intelligence*. Oxford: Oxford University Press. 2010. pp. 229, 230–241. doi:10.1093/oxfordhb/9780195375886.003.0014.

[6] Henricks S. C. Social Media, Publicly Available Information, and the Intelligence Community. *American Intelligence Journal*. 2017. 34 (1), pp. 21–31.

Facebook, LinkedIn, Instagram and Twitter), online discussion groups such as Reddit, bookmarking sites such as Pinterest, and E-Commerce such as Amazon; (3) public government data (e.g. government reports, budgets, hearings, telephone directories, press conferences, websites and speeches); (4) professional/industry/academic publications and commercial data (e.g. commercial imagery, financial and industrial assessments, and databases); (5) seized foreign material; (6) grey literature,[7] including foreign or domestic open source material that is usually only available through specialized outlets and may not enter normal channels or systems of publication, distribution, bibliographic control or acquisition by booksellers or subscription agents (e.g. technical reports, patents and business documents).[8]

It is important to note that open source information is not considered OSINT until 'it is analysed by an intelligence analyst in the context of national security requirements'.[9] Intelligence agencies can create OSINT either by having intelligence analysts do this work in-house, or by contracting it to outside entities (e.g. private companies, defence contractors, non-governmental organizations (NGOs) and academia).

Within the US IC, the use and importance of OSINT has varied. During the Cold War, it is thought that at times approximately 20% of US intelligence about the Soviet Union came from open sources.[10] Contemporary practitioners have arrived at higher estimates – that about 80–95% of US intelligence now comes from open sources (the 80% figure is most frequently mentioned).[11] It is not always clear how these percentages are arrived at, although some have noted that the higher figures are often cited for economic intelligence or information operations for which there is a

[7] National Grey Literature Collection. US Interagency Gray Literature Working Group Definition, 1995. Available from: http://allcatsrgrey.org.uk/wp/knowledgebase/u-s-interagency-gray-literature-working-group-definition-1995/ [Accessed 03 January 2022].

[8] For further discussion of categories of open sources, and how these relate to closed material, see also the chapter by H. Wilson *et al.* (Chapter 4.1).

[9] Saunders K. *Open Source Information – A True Collection Discipline*. MA thesis. Royal Military College of Canada. 2000. pp. 5, 26, 50, 105, 108–116, 120. Available from: https://docplayer.net/42068921-Open-source-information-a-true-collection-discipline.html [Accessed 03 January 2022].

[10] Lowenthal M. M. *Intelligence: From Secrets to Policy*. 4th ed. Washington, DC: CQ Press. 2009. p. 103.

[11] Mercado S. C. Reexamining the Distinction Between Open Information and Secrets. *Studies in Intelligence*. 2005. 49 (2). Available from: https://www.cia.gov/static/5d8a8df615f1bb014e49bb1452991991/Difference-Open-Info-Secrets.pdf [Accessed 28 July 2023].

large quantity of publicly available information.[12] Regardless, there is a widespread acknowledgement among intelligence experts that a sizeable amount of intelligence information now comes from open sources.

The US history of OSINT

Kimberly Saunders traced the first modern, institutionalized OSINT effort to the establishment in 1941 of the Office of the Coordinator of Information (COI). Launched before the United States joined the Second World War, this was the first peacetime, civilian, intelligence agency in the US (see footnote 9). A section called Research and Analysis (R&A) was set up within COI, which employed experts from several elite American universities and other subject matter specialists, who produced a variety of OSINT on enemy and allied countries. In 1942, the Office of Strategic Services (OSS) was created, which replaced the COI and provided a new base for the R&A branch (see footnote 9). Within the OSS, the R&A's main task was to provide strategic intelligence; to do this, its experts sought out and analyzed a wide variety of publicly available information from around the world. The R&A staff drew on their extensive expertise, experience and skills with open source research in academia to do their work, and developed a reputation among some that, 'R&A was the most important unit in the OSS' (see footnote 9). After the war, the OSS was abolished by Executive Order, and most of the researchers from the R&A unit returned to their universities.

In a distinct, parallel effort, the Foreign Broadcast Monitoring Service (FBMS) was created in 1941 under the Federal Communication Commission.[13] The mandate of the FBMS was to record, translate, transcribe and analyze propaganda radio programmes by the Axis powers – particularly those from Germany and Japan. After the Japanese attack on Pearl Harbor, and the US entry into the Second World War, FBMS changed its name to the Foreign Broadcast Intelligence Service, and the OSS relied on its work

[12] Saunders K. *Open Source Information – A True Collection Discipline*. MA thesis. Royal Military College of Canada. 2000. p. 50. Available from: https://docplayer.net/42068921-Open-source-information-a-true-collection-discipline.html [Accessed 03 January 2022].

[13] Mercado S. C. FBIS Against the Axis, 1941–1945: Open–Source Intelligence From the Airwaves. *Studies in Intelligence*. 2001. 11, pp. 33–43. Available from: https://www.cia.gov/static/96048eae9f1b9aa309a24c4b5582ea62/fbis-against-the-axis.pdf [Accessed 03 January 2022].

for various wartime assessments.[14] At the end of World War II, the Foreign Broadcast Intelligence Service was transferred to the War Department,[15] and then to the Central Intelligence Agency (CIA) where it was renamed the Foreign Broadcast Information Service (FBIS), and from where it monitored foreign media outputs.[16] FBIS became the central arm of the CIA's OSINT efforts during the Cold War. From the creation of the OSS until the 1990s, the bulk of open source analysis within the IC was scrutinizing and translating foreign press sources.

During the Cold War, the access to and use of open source information in the US declined, as the lowering of the Iron Curtain meant that many countries became closed to the West. This led the IC to depend more on information obtained through clandestine means, e.g. human sources (via spies) or classified technological systems. Because of this, the IC became increasingly structured around the collection and analysis of classified information, and OSINT was correspondingly de-emphasized. Analysts progressively relied upon (and became more trusting of) classified information for their assessments (see footnote 9).

Between the late 1980s and mid-1990s, with the advent of new information and communications technologies, the opening of previously closed Soviet bloc countries and the rise of various transnational threats, US intelligence began to recognize the growing availability of open source information and how it could be beneficial for intelligence assessments (see footnote 9, p. 5). In 1994, the CIA created the Community Open Source Program Office (COSPO)[17] to enable open source information to be more widely used within US intelligence. COSPO, however, failed to significantly change the existing reluctance to use, and overcome barriers to including,

[14] Mercado S. C. FBIS Against the Axis, 1941–1945: Open-Source Intelligence From the Airwaves. *Studies in Intelligence*. 2001. 11, pp. 33–43. Available from: https://www.cia.gov/static/96048eae9f1b9aa309a24c4b5582ea62/fbis-against-the-axis.pdf [Accessed 03 January 2022].

[15] Roop J. E. *Foreign Broadcast Information Service: History, Part I: 1941–1947*. Foreign Broadcast Information Service. April 1969 (Approved for Release 10 August 2009). pp. 110, 277–282, 298–307. Available from: https://worldradiohistory.com/Archive-FBIS/FBIS-History-First-Five-Years.pdf [Accessed 04 January 2022].

[16] *ibid*. p. 298–307.

[17] Director of Central Intelligence Directive 2/12: Community Open Source Program (Effective 1 March 1994). Available from: https://irp.fas.org/offdocs/dcid212.htm [Accessed 04 January 2022]. See also footnote 9, p. 4.

open source information within US intelligence.[18] From 1994–1996, the Aspin/Brown Commission on Intelligence Reform emphasized the need for the IC to increase its efforts to collect and use open sources, and to build more connections with outside subject matter experts.[19] In spite of this and other calls, by the end of the 20th century, the IC had failed to develop a meaningful capacity for OSINT.

The 11 September 2001 terrorist attacks on the United States led to a renewed focus on increasing OSINT by several legislators and intelligence managers. The Intelligence Reform and Terrorist Prevention Act of 2004[20] mandated the foundation of an Open Source Center (OSC), under the direction of the newly created post of Director of National Intelligence, to be managed by the CIA. In 2005, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission).[21] which was set up to examine the intelligence failures leading up to the 2003 Iraq War, also recommended creating an OSC within the CIA to ensure that the IC maximized the use of open source information.[22] Soon after, the Director of National Intelligence followed these suggestions and established the OSC within the CIA to be the centre of expertise on open source information for the entire US government. The CIA's previous open source research centre, FBIS, was subsumed within this.[23] However, despite this renewed focus on OSINT, former intelligence officer Arthur Hulnick writes, 'policy officials, the ultimate recipients of finished intelligence, were not quite as enthusiastic about OSINT as those who created the new system' (see footnote 5). In spite of the intelligence reform efforts post 9/11, OSINT continued to suffer, often being perceived as a lesser

[18] Lowenthal M. Open source intelligence: New Myths, New Realities. *Intelligencer*. 1999. 10 (1), pp. 7–9.

[19] Best R. A. Jr. *Open Source Intelligence (OSINT): Issues for Congress*. CRS Report for Congress. 28 January 2008. pp. 2–3, 9, 12. Available from: https://apps.dtic.mil/sti/pdfs/ADA488690.pdf [Accessed 04 January 2022]. See also footnote 10.

[20] Public Law 108–458—Dec. 17, 2004. *Intelligence Reform and Terrorism Prevention Act of 2004*. Available from: https://www.archives.gov/files/declassification/pidb/legislation/pdfs/public-law-108-458.pdf [Accessed 04 January 2022].

[21] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President.* 31 March 2005. p. 45. Available from: https://irp.fas.org/offdocs/wmd_report.pdf [Accessed 29 August 2023].

[22] Bean H. The DNI's Open Source Center: An Organizational Communication Perspective. *International Journal of Intelligence and CounterIntelligence*. 2007. 20 (2), pp. 240–257.

[23] Best R. A. 2008. *op. cit.*

intelligence discipline by the IC. To attempt to address this, in 2015, the OSC was redesignated the Open Source Enterprise and incorporated into the CIA's new Directorate of Digital Innovation, which is responsible for increasing the adoption of new digital tools and techniques across the CIA, to include cyber operations and OSINT.[24] The jury is still out as to how this reorganization has affected the status and use of OSINT within the IC.

The former Director of the OSC noted that although intelligence officials have increased their respect for and understanding of OSINT, financial constraints and competition among classified sources and platforms have hindered its uptake and progress.[25] As a result, over the years, eighteen IC members[26] have developed their own disparate OSINT operations, rather than engaging in a coherent, overarching OSINT policy and programme across the IC (see footnote 18). This has led to some concluding that OSINT is plagued by its 'persistent status as a subordinate intelligence discipline'.[27] This does not mean that OSINT has not garnered more representation and distinction over the years, but as one intelligence official has usefully commented on the state of play,

> I'd make a distinction between 'operationalized' and 'institutionalized.' 'Institutionalize' is very easy. Every agency has received a number of open source positions and resources. So, from an institutional standpoint, you can now identify open source officers in every agency in the intelligence community. . . . In terms of structure, I would say that this is first time in the history of the United States intelligence community that there are dedicated open source positions across the board. . . But in terms of operationalizing [open source intelligence], that's very different. We are still a long way from people looking at their business processes and saying, 'Ok, how do we inject open source in here?'[28]

[24] Aftergood S. Open Source Center (OSC) Becomes Open Source Enterprise (OSE). *Secrecy News*. 28 October 2015. Available from: https://fas.org/blogs/secrecy/2015/10/osc-ose/ [Accessed 04 January 2022].

[25] Bean H. The Paradox of Open Source: An Interview with Douglas J. Naquin. *International Journal of Intelligence and CounterIntelligence*. 2014. 27 (1), pp. 42–57. doi: 10.1080/08850607.2014.842797.

[26] US Department of Defense. USSF Becomes 18th Member of Intel Community. 8 January 2021. https://www.defense.gov/News/Releases/Release/Article/2466657/ussf-becomes-18th-member-of-intel-community/ [Accessed 04 January 2022].

[27] Bean H. 2014. *op. cit.*

[28] Bean H. *Constructing 'open source': Institutional discourse, cultural change & the post-9/11 reshaping of US intelligence*. PhD thesis. Boulder: University of Colorado. 2009. pp. 136–137, 192–193, 231.

Another OSINT proponent has surmised that 'The real sign that open source [intelligence] has arrived is when an independent agency is created to pursue open source, to train open-source disciples, to promote it within the different agencies of the intelligence community. We're not there yet'.[29] Other intelligence scholars and practitioners have also called for this reorganization.[30] To date, OSINT and its various roles, scope and authorities have been repeatedly deprioritized and under-resourced within the IC.

Intelligence Culture and OSINT

Many intelligence scholars and practitioners have noted that the problems with increasing the role, practice and prominence of OSINT within the IC stem from the culture among intelligence officials, managers and analysts, which – since the Cold War – has valued and prioritized classified information and classified collection systems.[31] In part, this is because the collection and use of classified information has been what makes the US intelligence community special and distinct from other government and non-government entities. Former Assistant Deputy Director of National Intelligence for Open Source Eliot Jardines sums this up, saying, 'Let's keep in mind that we in the intelligence community take pride in knowing things or having the ability to know things that others don't, and so there's just the natural tendency that if the document's got a fancy cover sheet that says Top Secret and all sorts of fancy code words on it, that we tend to view that as more important than, say, something that's taken just from open sources' (see footnote 29, p. 136). Some argue that there is also competition within the IC between proponents of classified documentation and OSINT advocates, with the latter maintaining 'that there is no question that the secret side has interfered with the development of a full and complete open source capability' (see

[29] Bean H. *Constructing 'open source': Institutional discourse, cultural change & the post-9/11 reshaping of US intelligence.* PhD thesis. Boulder: University of Colorado. 2009, pp. 192–193.

[30] Zegert A. and Morell M. Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail. *Foreign Affairs*. May–June 2019. 98(3), pp. 85–96. Available from: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/zegartmorell.pdf [Accessed 4 January 2023].

[31] Lowenthal M. Open Source Intelligence: New Myths, New Realities. *Intelligencer*. February 1999. 10(1). pp. 7–9.

footnote 29, pp. 136–137). Others have noted a less sinister reason; the IC responds to the collection priorities laid out in the National Intelligence Priorities Framework (NIPF)[32] – and the IC's solutions for addressing this mostly consist of using classified technological systems that result from decades of large investments.[33] As one former Director of Central Intelligence (DCI) stated, 'I only have money to pay for secrets'.[34] Thus, funding priorities continue to focus on classified platforms and investments in new classified collection technologies.

Persistent challenges

This prioritization has also been shaped by policy-officials and other intelligence customers who tend to want 'material from spies, intercepts, or any of the other more exotic material available to intelligence analysts' (see footnote 19, pp. 2–3). Otherwise, they claim, reading intelligence analysis is no different from reading the daily newspapers (see footnote 5, p. 230). As noted above, the intelligence failures leading up to 9/11 created an opening for OSINT, but the IC has still failed to overcome its inherent preference for classified information (see footnote 29, pp. 136–137). Intelligence scholars Tore Pedersen and Pia Therese Jansen recently conducted a randomized controlled trial in which they found that, in certain instances (detailed below), intelligence analysts significantly assign more credibility to secret information, even when the secret and open sources are identical.[35] Similarly, they found that intelligence analysts are considerably more confident in assessments when they are based on classified information versus identical analysis based on open source information. Interestingly, Pedersen

[32] Office of the Director of National Intelligence. *Intelligence Community Directive 204: National Intelligence Priorities Framework*, 7 January 2021. Available from: https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf [Accessed 4 January 2022].

[33] Weinbaum C. The Intelligence Community's Deadly Bias Toward Classified Sources. *The RAND Blog*. 12 April 2021. Available from: https://www.rand.org/blog/2021/04/the-intelligence-communitys-deadly-bias-toward-classified.html [Accessed 4 January 2022].

[34] Marks R. A. Spying and the Internet. *The Washington Times*. 25 April 2005. p. A–21. Available from: https://www.washingtontimes.com/news/2005/apr/24/20050424-101721-8924r/ [Accessed 4 January 2022].

[35] Pedersen T. and Jansen P. T. Seduced by secrecy — perplexed by complexity: effects of secret vs open-source on intelligence credibility and analytic confidence. *Intelligence and National Security*. 2019. 34(6), pp. 881–898. Available from: https://doi.org/10.1080/02684527.2019.1628453.

and Jansen found that these results only applied to cases when the intelligence estimate corresponded to a 'complex' problem characterized by a high degree of uncertainty, and not when the estimate addressed a 'simple' problem characterized by a low degree of uncertainty. They surmise that these results could be explained by the fact that intelligence analysts have tended to work more with classified information than with open source information, or because they do not have the time or resources to carefully vet the open source information. This can lead to what Luis Garciano and Richard Posner call the 'herding problem' in intelligence, in which analysts can tend to focus on the same limited, classified information when making their assessments. This herding problem often gets 'locked in' because of the privileging of classified collection systems and information.[36]

However, despite this apparent resistance to OSINT in the IC, there are internal advocates promoting its importance and use. Some argue that open source information can be instrumental in helping analysts to narrow and define the scope of classified collection and analysis, and can provide important contextual understanding of classified data.[37] One useful case in point comes from the work of Professor Flagg Miller, a linguistics anthropologist and religious studies scholar, who analyzed over 1,500 cassette tapes from Osama bin Laden's former home in Kandahar, Afghanistan, after the fall of the Taliban in 2001 (the FBI had vetted the cassettes, deemed them insignificant, and then donated them to Williams College, thereby making them open sources).[38] Through careful study of these tapes, underpinned by his expertise in public domain literature, Miller worked to understand why bin Laden and his followers engaged in terrorist activities. His analysis of these tapes revealed a fundamental misunderstanding in the West's characterizations of bin Laden's activities as being a transnational, anti-American terrorist network. Rather, Miller found that in the 1990s bin Laden and his Al

[36] Garciano L. and Posner R. A. Intelligence failures: An Organizational Economics Perspective. *Journal of Economic Perspectives*. 2005. 19 (4), pp. 151–170.

[37] Davitch J. M. Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data. *Joint Force Quarterly*. 2017. 87, pp. 18–25. Available from: https://ndupress.ndu.edu/Publications/Article/1325926/open-sources-for-the-information-age-or-how-i-learned-to-stop-worrying-and-love/ [Accessed 04 January 2022].

[38] Miller F. *The Audacious Ascetic: What the Bin Laden Tapes Reveal About Al-Qa'ida*. Oxford: Oxford University Press. 2015.

Qaeda organization were focused on what they saw as apostates of the Muslim world, and on winning religious and political battles within Muslim-majority societies. Bin Laden's later targeting of America was built on western security discourse and narratives that he exploited when he understood there was political capital in doing so. This kind of nuanced understanding of bin Laden and his affiliates, based on open source information and analysis of these audio cassettes, could have led to a very different kind of intelligence assessment and set of policy responses towards Al Qaeda's activities during the 1990s and early 2000s.

Beyond these kinds of contextual studies, others say that open source information, and OSINT, has value as an intelligence discipline in and of itself. Former OSC analyst Stephen Mercado argues that OSINT beats classified information in terms of speed, quantity, quality, clarity, ease of use and cost, and that it 'often equals or surpasses secrets in addressing such intelligence challenges of our day as proliferation, terrorism, and counterintelligence' (see footnote 13). He and his fellow OSINT advocates, however, have not managed to penetrate the IC's longstanding preference for classified information and classified systems.

Some intelligence practitioners have pointed out that intelligence managers can play an important role in overcoming these internal barriers to OSINT.[39] Former IC practitioner John Gentry describes analytic managers as 'barons' who are the key decision-makers on a given analytic product/project and thus decide 'who and what gets to play' on a given issue.[40] Therefore, if IC managers are vested in OSINT, this can translate to analysts working more with open source information and producing OSINT. This could work separately from, or in tandem with, ongoing calls for structural changes and reforms within the IC to promote OSINT.

New challenges

While the IC has been slow to fully incorporate open source information and OSINT into its practices, the rise of private companies and non-government

[39] Gentry J. A. Managers of Analysts: The Other Half of Intelligence Analysis. *Intelligence and National Security*. 2016. 31 (2), pp. 154–177. See also footnote 27.
[40] *ibid.*

entities, and the creation of an OSINT market, may force it to reconsider its longstanding preference for classified sources and systems. Over time, because of dissatisfaction with IC assessments, policy-makers and other intelligence customers have turned to OSINT from outside groups.[41] This was noted particularly during the George W. Bush administration, in which then Under Secretary for Defense Policy, Douglas Feith, set up intelligence gathering and analytic entities within the Department of Defense to gather information and conduct assessments to rival the IC's assessments on the Iraq–Al Qaeda relationship.[42] In addition, others would point out that the ongoing digital technology revolution is putting more and more information about the outside world directly into policy-makers' hands in near real time, giving them the feeling that they do not have to depend on the IC to acquire and understand information on important world and security developments.[43] Over the past few decades, the IC has had to compete for policy-makers' attention with 24-hour news media and instantaneous communication via social media, as well as other online platforms. Some have raised concerns that this may encourage policy-officials to rely on raw data (that has not been authenticated and assessed), and may tempt some officials to conduct their own analysis (see footnote 28). In this world of instant information, intelligence analysts will need to provide added value and context, beyond what is easily available to policy-makers, and the value of OSINT will be in the analysis of such raw data.[44] Marcos Degaut argues that now and in the years to come, the IC is and will be competing with a complex and diverse group of domestic and foreign information collectors, brokers and analysts providing information almost instantaneously as events happen,[45] the veracity of which must be

[41] Sands A. Integrating Open Sources into Transnational Threat Assessments, in Sims J. E. and Gerber B. (eds). *Transforming U.S. Intelligence*. Washington, DC: Georgetown University Press. 2005. pp. 63–78.

[42] Pincus W. and Smith R. J. Official's Key Report on Iraq is Faulted. *The Washington Post*. 8 February 2007. Available from: https://www.washingtonpost.com/wp-dyn/content/article/2007/02/08/AR2007020802387.html [Accessed 9 August 2023].

[43] Degaut M. Spies and Policy-makers: Intelligence in the Information Age. *Intelligence and National Security*. 2016. 31 (4), pp. 509–531. doi: 10.1080/02684527.2015.1017931.

[44] Duvenage M. *Intelligence Analysis in the Knowledge Age: An Analysis of the Challenges Facing the Practice of Intelligence Analysis.* Stellenbosch, South Africa: Stellenbosch University. 2010.

[45] *ibid.*

vetted and may need to be challenged. This information environment is far different to that operating during the Cold War and immediate post-Cold War period, in which the IC had essentially a monopoly of policy-makers' attention on security developments.

In light of this changing environment, some have suggested that the IC must devote more internal human and technical resources to OSINT (see footnotes 11 and 25). Others would argue that – given the recent rise in non-governmental OSINT – it is already too late for this, and that instead, the IC must create new external partnerships with industry, academia, and other groups and individuals that already have the expertise needed to conduct OSINT. Since the late 1990s, several OSINT businesses and consultants, often former intelligence practitioners, have set up shop as 'information middlemen' (see footnote 43) to provide this kind of service to the IC (see footnotes 5 p. 231, 22 p. 247, and 28 p. 4). These entities have grown with the proliferation of information from the internet and various social media and online sources, as well as with the reduction of the IC work-force in the post-Cold War 'peace dividend' period.[46] Contracting with and/or outsourcing to private-sector companies to collect and analyze open source information has become a way for the IC to manage the growing big data/information burden. Tim Shorrock has called the rise of these arrangements the 'Intelligence-Industrial Complex'.[47] There are concerns about these developments, with some arguing that the IC should not out-source work that it has no competency to evaluate (see footnote 25, p. 51). It should be noted that as the number of these non-governmental entities and their capabilities grow, they will have a growing financial stake in how OSINT is defined and managed, and they will increasingly shape the ongoing debate on the IC's relationship with OSINT now and into the future.

Regardless of whether and how the IC handles OSINT now or later, there are additional challenges that arise with a move towards more OSINT. The use of commercially available datasets by the IC has raised questions about

[46] Shorrock T. *Spies for Hire: The Secret World of Intelligence Outsourcing*. New York: Simon & Schuster. 2008.
[47] *ibid.*

privacy protections of US citizens. In one example, the IC collected and analyzed location data from smartphone apps from a commercial, third-party information broker, to scrutinize the movements of US citizens without a warrant.[48] According to a 2018 Supreme Court ruling, the IC is required to obtain a warrant in order to compel phone companies to turn over location data about their customers.[49] However, the IC and other government agencies can purchase similar data from commercial information brokers, and the law is unclear about whether a warrant is needed for this. The proliferation of third-party, commercial information brokers across various communication technologies, as well as through online and social media platforms, raises continued questions about the IC, OSINT and privacy protections in the digital age.

The proliferation of online open source information also raises analytic challenges in terms of sorting through misinformation, disinformation and algorithmic biases.[50] In this context, Nicole Softness raises the issue of 'context collapse',[51] whereby social media messages or posts originally meant for a small, specific audience might be misconstrued once accessed by a larger audience. She and others[52] further point out that analyzing these kinds of online posts cannot reveal the intentions or motivations of an actor or group (some of whom may deliberately try to mislead), yet some OSINT attempts to make just such a determination. Therefore, expertise and quality

[48] Savage C. Intelligence analysts use U.S. smartphone Location Data without Warrants, Memo Says. *The New York Times*. 22 January 2021; updated 25 January 2021. Available from: https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html [Accessed 9 August 2023].

[49] Liptak A. In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy. *The New York Times*. 22 June 2018. Available from: https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html [Accessed 9 August 2023].

[50] Rønn K. V. and Søe S. O. Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*. 2019. 34(3), pp. 362–378. Søe S. O. Misleadingness in the Algorithm Society: Misinformation and Disinformation. *Medium*. 6 March 2017. Available from: https://medium.com/big-data-small-meaning-and-global-discourses/misleadingness-in-the-algorithm-society-misinformation-and-disinformation-28f78f14e78f [Accessed 9 August 2023]. Søe S. O. Algorithmic Detection of Misinformation and Disinformation: Gricean Perspectives. *Journal of Documentation*. 2018. 74(2), pp. 309–332. Available from: https://www.emerald.com/insight/content/doi/10.1108/JD-05-2017-0075/full/pdf?title=algorithmic-detection-of-misinformation-and-disinformation-gricean-perspectives.

[51] Softness N. A. Social Media and Intelligence: The Precedent and Future for Regulations. *American Intelligence Journal*. 2017. 34 (1), pp. 32–37.

[52] Rønn K. V. and Søe S. O. Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*. 2019. 34 (3), pp. 33, 362–378.

control are needed to sort through the veracity of open source information, as well as the analytic methods used to process it and make sense of it.[53]

Finally, the increasing algorithmic mining of open source information also raises questions of how to think about the role of the intelligence analyst vis-à-vis these digital technologies, regardless of whether OSINT is conducted in-house or outsourced. Typically, assessments of the potential of OSINT have tended to have a technocratic focus, for example, examining new technological capabilities which many hope will enable the mining of more diverse open source information and larger datasets.[54] Instead, some argue that it would be better for the IC to start by asking precisely what intelligence questions need to be answered, and then considering which resources and methods are best suited to answering these, which could include a combination of different sources of information, analytic techniques, analyst expertise and skill sets, as well as software and technologies. Former Director of the Open Source Center Douglas Naquin argues that 'Technology and statistical analysis should allow us to organize haystacks better, but I believe we will still depend on substantive – and Open Source – experts to derive insight from those haystacks, let alone find any needles' (see footnote 25). Some intelligence scholars and practitioners argue that in this context, rather than focusing on the technology, the IC should focus on hiring more subject matter experts, creating partnerships with outside experts, and developing more analytic standards and methods in the use of human judgment, to help inform and interrogate OSINT collection and analysis.[55],[56] Others have also pointed to how intelligence analysts need more

[53] Haggerty K. D. and Ericson R. V. The Surveillant Assemblage. *The British Journal of Sociology*. 2000. 51(4), pp. 605–622. See also footnote 25, p. 50.

[54] Eldridge C., Hobbs C., and Moran M. Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data'. *Intelligence and National Security*. 2018, 33 (3), pp. 391–406. Available from: https://doi.org/10.1080/02684527.2017.1406677. See also footnote 18 and 25 p. 49.

[55] Several chapters in this volume consider non-governmental research that uses hybrid approaches, that span both open and closed sources, and provide examples of non-governmental open source research correcting official accounts. For example, see chapters by Wilson, Samuel & Plesch, Strick, Kristensen & Korda, Triebert, and Carboni & Raleigh (Chapters 1, 2.1, 2.3, 2.4 and 3.3).

[56] Eldridge C., Hobbs C. and Moran M. Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data'. *Intelligence and National Security*. 2018. 33(3), pp. 391–406. Lim K. Big Data and Strategic Intelligence. *Intelligence and National Security*. 2016. 31(4), pp. 619–635. See also footnote 25 p. 48, and footnote 51 p. 37.

training, as well as access to unclassified sources, tools and platforms, in order to better understand how to effectively collect and analyze open source information.[57]

Conclusion

OSINT has had a long and varied history within the US IC. For much of this time, however, OSINT has been subjugated within intelligence practices. Rather than having a focused, coherent policy and programme, OSINT has tended to be scattered across different intelligence organizations, and the community has been inclined to underfund OSINT and instead favour intelligence that originates from classified sources.

However, the ongoing information revolution has started to challenge this, by giving rise to external information brokers and private OSINT entities that are putting pressure on the IC to consider how to best integrate open source information and intelligence into its structures and practices. OSINT is challenging traditional notions of what constitutes 'intelligence', and what makes the 'intelligence community' distinct from other government or non-government analytic bodies. Meanwhile, OSINT conducted by non-governmental groups is demonstrating that it can achieve results quickly, cheaply and accurately, and that it can complement and enhance intelligence based solely on classified sources.

The US IC's traditional resistance to OSINT has 'deep roots' (see footnote 5), and it is likely that a paradigm shift will be needed to change this (see footnote 25, p. 46). This will require strong, sustained, high-level internal advocates across IC management levels, as well as larger cadres of analysts who have expertise in how to use OSINT effectively. It remains to be seen how various social factors internal and external to the IC will shape the influence of OSINT in the years to come. This will be a space that is interesting to watch.

[57] Weinbaum C., Parachini J. V., Girven R. S., Decker M. H., and Baffa R. C. "Perspectives and Opportunities in Intelligence for U.S. Leader". September 2018. Available from: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE287/RAND_PE287.pdf [Accessed 29 August 2023].