International Journal of Intelligence and CounterIntelligence

ISSN: 0885-0607 (Print) 1521-0561 (Online) Journal homepage: https://www.tandfonline.com/loi/ujic20

Open Source Intelligence (OSINT): An Oxymoron?

Bowman H. Miller

To cite this article: Bowman H. Miller (2018) Open Source Intelligence (OSINT): An Oxymoron?, International Journal of Intelligence and CounterIntelligence, 31:4, 702-719, DOI: 10.1080/08850607.2018.1492826

To link to this article: https://doi.org/10.1080/08850607.2018.1492826

International Journal of Intelligence and CounterIntelligence, 31: 702–719, 2018

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2018.1492826

BOWMAN H. MILLER

Open Source Intelligence (OSINT): An Oxymoron?

> *Open-source was "frosting on the cake" of intelligence material dominated by signals, imagery, and human-source collection. Today, open source … comprises a large part of the cake itself.*
>
> —John C. Gannon, former Deputy Director of CIA for Analysis[1]

In today's world information of all kinds is available to anyone who cares to see it. If that's the case, can such publicly accessible information be considered intelligence? The answer is: "It depends." A conundrum facing U.S. intelligence is the enormous spectrum of information broadly known as "open source." As countless commentators repeat the shopworn claim that the world is changing in ways and at a pace never before seen, have the role and definition of intelligence remained what they were in the last millennium? If not, what makes "OSINT," its sources and its functions, different from what intelligence was during wars from World War II to Korea and Vietnam, in various crises from the Cold War and the Cuban Missile Crisis, and more recently in light of the 11 September 2001 (9/11) attacks, Iraq, Afghanistan, and the unseasonably short-lived "Arab spring"? While the world has changed dramatically over the last quarter-century, has the explosion of open source information changed the definition and expectations of intelligence?

Dr. Bowman H. Miller teaches at the National Intelligence University after a career in the U.S. Air Force and in the U.S. Department of State, where he served as Director of Analysis for Europe, 1987–2005. The views expressed in this article are those of the author and do not reflect the official policy or position of the National Intelligence University, the Defense Intelligence Agency, the Department of Defense, the Department of State, or the U.S. Government.

One element of the current information reservoir that is indeed vastly larger and more prevalent is what has come to be called OSINT—"open source intelligence." Intelligence has seen its information challenge transformed from coping with paucity to confronting saturation. While the importance of openly accessible information in understanding the world and its many elements cannot be denied, and has long been a staple of information gathering and all-source analysis, can information that is freely accessible or simple to buy automatically be characterized as "intelligence"? Moreover, how does and should "OSINT" relate to and buttress the broader intelligence collection and analysis enterprise?

DEFINING INTELLIGENCE

If today's intelligence is comprised of upwards of eighty percent open source information, can OSINT be disqualified as an intelligence discipline? If so, how and why? What, after all, is intelligence? Former intelligence official Mark M. Lowenthal begins his book *Intelligence: From Secrets to Policy* with that question. His first answer is:

> Intelligence refers to information that meets the stated or understood needs of policy makers and has been collected, processed and narrowed to meet those needs. Intelligence is a subset of the broader category of information. … All intelligence is information; not all information is intelligence.[2]

This utilitarian definition, like many others, tends to focus on the intelligence function over form, while making no reference to secrecy. That definition's last element, placing intelligence as a subset of information, is central to the OSINT issue. Lowenthal later added: "By *open-source information*, we mean any and all information that can be derived from overt collection … ."[3] [*Emphasis in original*.] In *Reducing Uncertainty*, Thomas Fingar, a former Chairman of the National Intelligence Council, asserted that "[t]he purpose of intelligence since time immemorial has been to reduce uncertainty about the aspirations, intentions, capabilities and actions of adversaries, political rivals, and, sometimes, partners and allies."[4] The coinage, attributed to former State Department intelligence official Jennifer Sims,[5] of seeking (by means of intelligence) to provide "decision advantage" to the policy and decisionmaker also emphasizes use over origin. Elsewhere, Sims defines intelligence as "information collected, organized, or analyzed on behalf of actors or decision makers."[6] Again, her focus is on intelligence's aims, not its means of acquisition.

Is OSINT then just another example of the inescapable American government and cultural obsession with acronyms? Or does it anticipate what happens when open source information takes on an intelligence role—and

gets classified in the process? Does it belong in the pantheon of existing INT-disciplines, such as human intelligence (HUMINT) and the others? If OSINT is public or readily accessible information or data, what enables its classification as "intelligence"? These functional perspectives on intelligence provide part but not all of the answer. They are useful in looking at intelligence in terms of the purposes for which it is sought, acquired, processed, analyzed, and distributed. But this mission focus is not what primarily characterizes the particular INT-disciplines that make up the business of collecting intelligence: signals intelligence (SIGINT), human-derived intelligence (HUMINT), geo-spatial/imagery intelligence (GEOINT or IMINT), and measures and signatures (sensor-derived) intelligence (MASINT).

Each of these collection disciplines is typified by the need to target certain specific kinds of information to fill particular information (or warning) needs by using special, concealed methods to collect that information. Those means are applied against a range of targets and types, be they countries, leaders, terrorist groups, drug cartels, human traffickers, weapons systems, decision processes, or covert plans, to name some of the more prominent concerns. But each such "INT" denotes a particular set of methods, sources, and, at times, technologies employed to secretly acquire information that others seek to conceal—and then to hide its secret possession from them and others lacking the proverbial "need to know." Those who know they have been penetrated can change plans, alter codes, engage in deception, bury reactors, or otherwise defeat sources and methods used against them. What is most sensitive regarding the traditional collection "INTs" are the capabilities of their varied methods and sources. Regardless of its origin and content, intelligence loses some, if not most, of its value if and when it becomes public. And publicizing intelligence always raises the risk that the utilized sensitive sources and methods will become known and their effectiveness compromised, the concern that lies at the heart of the dyspepsia over intelligence leaks. That said, policy and national interests are occasionally served by strategically divulging some aspects of otherwise secret intelligence, for example, information regarding the Soviet missiles in Cuba, the Chernobyl reactor meltdown, war crimes and mass graves, natural disasters, and such.

IF IT'S FREE, WHY STEAL IT?

Beginning in 1992, a new emphasis on exploiting open sources for potential intelligence value developed, with congressional calls for such a focus, along with a reform of the U.S. Intelligence Community (IC) to accomplish it. After all, acquiring openly available information entails less cost and less risk but can provide the baseline of information on which to build by using other,

sensitive collection methods. In 2005, after 13 years in gestation, the Director of National Intelligence's (DNI) Open Source Center (OSC), managed by and housed in a Central Intelligence Agency (CIA) facility, was finally inaugurated. It was built on the structure of the former Foreign Broadcast Information Service (FBIS), a critical asset for analysts, academicians, and others during the Cold War, when access to the Communist world and its propaganda output—the real precursor of "fake news"—was much harder to come by.

Today, the OSC employs "collectors" of a type radically different from the case officers of the CIA's clandestine service. They do not collect in the same sense; rather, they identify, sift, and exploit information. But, unlike other intelligence disciplines, open source acquisition must wait until someone else has created the information. Much of what these "open source collectors" do resembles the work of a research librarian, whose tasks also include discovering new, viable, and informative sources and research products. That involves both search and assessment, but it consists of identification, not collection. On its Internet website the OSC outlines the following basic responsibilities and functions of an "open source collection officer":

> Open Source Collection Officers (OSCOs) are responsible for systematically collecting publicly available information in a given region or a subject area to meet customer needs. The information is known as Open Source Intelligence (OSINT) and includes traditional mass media, the internet, specialized journals, studies, conference proceedings, geospatial information, and more. OSCOs develop strategies and plans for the collection of OSINT, including the tools and methodologies needed to accomplish the task:
>
> Drive integrated information gathering on a strategic topic, regional, or cross-regional need;
>
> Research and acquire publically [sic] available information in response to intelligence gaps;
>
> Identify relevant sources for data collection.[7]

In short, open sources do not have to be discovered, recruited, intercepted, or sensed technologically in the manner of clandestine modes of collection. Rather, open source "collectors" must scan the horizon for valid sources, then screen, sort, filter, and acknowledge them as both accurate and relevant, or otherwise discredit them. Factual nuggets must be separated from the piles of ore that make up most of the openly available information blanketing the world every minute of the day. (Notably, in the published job description for OSC collection officers, the IP address contains no reference to collection per

se but instead to an "analytical" role.)[8] The OSINT collector-analyst connection is much closer than those in the other INTs, with GEOINT perhaps coming in second in this respect.

Given the current physical and organizational locus of the Open Source Center, the ancillary concern arises that a bureaucratic culture that emphasizes secrecy to the hilt (i.e., the CIA) will want to restrict with classified markings even open source and openly-acquired information. This tendency to privatize publicly available information is not only inappropriate but also ineffectual. It is an "operation barn door," with the open source horse having already left the stable. Nonetheless, all too often those focused on clandestine tradecraft want to do just that. Whether open source management and exploitation deserves to be a separate, single IC agency is a related topic for others to tackle.[9] But its appropriateness and effectiveness, not to mention the likelihood of even more bureaucratic overkill, can be seriously questioned. George Orwell would not be surprised.

Open source information is only information, unless or until it is used to fill an intelligence need or serve an intelligence purpose. Thus, OSINT varies not only in its acquisition but in its transformation from information into a role as intelligence. An official OSINT definition asserts:

> Open-Source Intelligence (OSINT) is intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. OSINT draws from a wide variety of information and sources, including: mass media; public data; gray literature; and observation and reporting.[10]

Apparent from this definition, perhaps better called a description, is that OSINT can and does cover a multitude of methods and venues. But a peculiarity of OSINT is that the clandestine collection disciplines also tend to have their open source counterparts. Thus, GEOINT has an increasing number of commercial alternatives in DigitalGlobe, Google Earth, MapQuest, and more. Whether those imagery producers should be better labeled as providers of GEOINT or of OSINT is a matter of debate. Much of this geo-referenced information is there for the asking, perhaps from a laptop computer at the neighborhood Starbucks. Of course, doing this research also allows the seeker's location to be recorded and tracked. And this kind of information can be purchased in the open market. Television and social media serve in many ways as publicly-relayed avenues of SIGINT, and often as real time streaming video. Malevolent forces use the Internet and social media to propagate hatred, advertise recipes for fabricating explosives and various attack methods, recruit partisans, and communicate directives. And those open uses call for their identification and exploitation as intelligence.

Some aspects of MASINT also amount to open source data. Such can be found in seismometers routinely measuring earthquakes and in sensors measuring airborne radiation, indications of nuclear tests, or reactor calamities. Much of this data is available from the National Weather Service and National Oceanographic and Atmospheric Administration (NOAA). Indeed, in a sense every device able to communicate and to access the Internet has become a sensor for the person using it. Democratization in access to technology gives every user the power to create information, make news, and shape opinions as never before. Most journalists carry out a form of public HUMINT as they acquire and make use of sources, some of them most useful when anonymous, while others are openly named.

Taken together with the broad range of other public sources of information, the OSINT phenomenon shows itself to be a hyper-federated reality,[11] spanning untold sites and methods. Knowing few bounds, it also reflects a speed that is often spell-binding: the rapidity of posting something on the Internet coupled with the ability to remove it in an instant. But do this ubiquity, rapidity, and variety provide the basis for characterizing open source as a distinct INT?

UNEARTHING SECRETS VS. FILTERING INFORMATION

Practitioners of the craft of intelligence focus heavily on specialized, protected sources and methods of intelligence acquisition, using primarily clandestine means. The purists' understanding of intelligence—widely held, especially among collectors—consists of information held in secret by others that is surreptitiously acquired using hidden methods, protected from disclosure, and put to use secretly by recipient decisionmakers. Unlike OSINT, these varieties of information are not "hidden in plain sight." Moreover, OSINT's entirety is comprised of secondhand information—also true for much of SIGINT—but in the latter case speakers/targets are not aware that they are being monitored. Some other person or entity originated the OSINT information. And, for it to be labelled OSINT in U.S. intelligence parlance, it must have been legally acquired.[12] And legally acquired also means that copyright and patent protections must be observed. (Even in the realm of acquiring foreign military materiel, the U.S. government simply buys what it can before resorting to other, more nefarious methods of acquisition.) Not so with clandestine collection. Thus, selected targeting and clandestine collection contrast starkly with assembling the masses of publicly accessible or purchasable information openly cascading daily around the globe on widely accessible systems.

In both cases, those useful nuggets of information are sought in an effort to answer questions, fill intelligence gaps, and reduce uncertainty for decisionmakers. In using clandestine techniques, the issue is target

identification and target access. In OSINT, target identification is equally relevant, but the issue of access is different. It has less to do with collection and much more to do with the acquisition and sifting of masses of information—justifying the cliché of trying to minimize "drinking from a firehose." Indeed, the looming danger today is that key kernels of secret intelligence can drown in the flood of open source information. As the historian of intelligence Ernest May has observed, "[T]he galloping information revolution [has] strained the capacity of the intelligence community to perform its traditional function of providing policymakers with information not obtainable from open sources."[13] Obtainable from open sources, if well selected and well used, is sense-making data. Those sources can provide context, perspective, alternative interpretations, and world views, what the Germans call *Weltanschauung*.

Identifying and accessing the target is the critical component of clandestine collection methods. A time-worn cliché regarding intelligence collection holds it to be an analysis-driven process, meaning that intelligence analysts point collectors to what both they and their consumers need and are missing in order to give warnings or make judgments. Among all-source analysts, experience shows that such an "analysts-guiding-collectors" process is more fiction than reality. Indeed, many clandestine HUMINT collectors, exploiting either human or technical sources, see little, if any, value in analysis. They are loathe to pay homage to the analyst as the reputed driving force behind the collector's work, and often pay little heed to what analysts claim to want or need.[14] Indeed, a more accurate portrayal of the relationship between collectors and analysts, although somewhat exaggerated, has been that "never the twain shall meet."[15] But in OSINT analysts, rather than operators/collectors, tend to write the requirements.

OSINT: A COLLECTOR-FREE DISCIPLINE?

When clandestine case officers seek to enlist secret human sources, they engage in complicated, risky, time-consuming tradecraft: spotting, assessing, and vetting the person they target for potential recruitment to determine his/her bona fides, access, susceptibility, and reliability. When the Intelligence Community engages in technical collection, that too is carefully calibrated to get the best, most critical, and most useful information to policymakers and war fighters. How does that assessment and prioritization process work when dealing with open source information? Do analysts tend to be overwhelmed by the volume of open source and social media information and communications? How adept is technology at sorting through trillions of messages daily to find that "needle among a stack of needles" that affords the intelligence consumers a "decision advantage" and reduces their uncertainty?

While collection is the key in the traditional, concealed INT-disciplines, for OSINT it is identification, validation, and exploitation. OSINT is more an acquisition search than a collection targeting. But finding what is useful, timely, and relevant in the vast reservoir of open source information is a task for neither amateurs nor many analysts. In the arena of open source information inquisitive analysts can call more of the shots, and perform a role more closely related to that of collector. Many analysts remain wary of those who intervene between them and original sources, even translators in some cases. But the typical analyst is not well-versed on how and where to seek in open sources what is needed and lacking. Moreover, much of what is useful is often harder to find, is not in English, and is part of a seemingly impenetrable mass of data and streaming information. More and more of it no longer appears as text. This accounts for why the OSC uses individuals who are better qualified to understand local languages, customs, perspectives, narratives, and priorities.

Thus, even if some analysts can parse open source databases on their own, doing so is both time-consuming and often imprecise. Open source searches do not involve simply surfing the World Wide Web. Such inquiry demands the skills, knowledge, and inquisitiveness of a research librarian. While they may be able to circumvent the need for and functions of collectors, searching for information is not the bread and butter of most all-source analysts. This holds true even if all analysts were to also act as investigative researchers, and they should not be confident that what they need will almost magically appear on their computer screens. They, or those who support them in the world of OSINT, need to know what avenues and reservoirs of information and perspective can be of value for the areas that they cover, and where and how to exploit them.

TAPPING FOREIGN SOURCES FOR "GLOBAL COVERAGE" CONTENT AND FOR CUEING

Open source information simply exists, and in ever-growing masses. The task, then, is not so much to acquire open source data and communications, but more to winnow its bulk down to what holds promise for intelligence value before acquiring or assessing it. The open source screener must sort and sift for that minute fraction of the information universe that can serve an intelligence purpose. And those purposes are essentially threefold: (1) obtaining information with valuable, intelligence-relevant content per se; (2) building and deepening analysts' knowledge base; and (3) discovering information that can be used indirectly to cue one of the clandestine intelligence disciplines toward a target or a concern, or to unearth more detail on a target of interest. Often, those clandestine means are necessary to scrutinize and validate something reported publicly, whether in news

coverage, via social media, or otherwise. That kind of open reporting, often instantaneous, also comes without authentication. OSINT demands attention to denial and deception measures every bit as much as do traditional collection disciplines. Any astute Internet user is vigilant when it comes to phishing, hacking, fake data, scams, and the like—an ever-present cyber security concern in the OSINT arena.

The cueing function of open sources often proves of great value. Examples include the global ubiquity of social media and peoples' ability with their cellphones to photograph in real time such events as a protest in progress, a terrorist incident, or a natural disaster. That same information can be relayed to geospatial collectors, whether governmental or commercial (e.g., DigitalGlobe), for them to examine and report on, using their unique, often wider-ranging, and proven credible capabilities. This kind of information gathering symbiosis holds in many other areas—tracking human and drug trafficking routes, detecting hostile efforts at denial and deception, identifying cyber intrusions and distortions, and more. Often the process of validating the trustworthiness of an open source's data requires scrutiny using classified, sensitive collection and targeting methods. If the two conflict, analysts must find ways to decide which to believe and use in making their judgments.

The reverse in the pointing context also occurs, when clandestinely acquired information helps direct, target, locate, and/or sort open source information or communication. Purposely concealed traffic on the Internet that cannot be accessed without special or concealed techniques remains in the domain of clandestine collection, e.g., in the "dark web," but the public's open tweets, blog entries, published journals, and such qualify as accessible open sources. The world of information, massive and molten as it now is, requires advanced data analytics, adroit human screening, and schooled analytic judgment in order to determine what is to be sought out, believed, included in analysis, or discredited and discarded.

LEARNING FOREIGN REALITY FROM FOREIGNERS

One paradox of using open sources to better understand the larger world and its many players and facets is the matter of gaining the most useful and relevant information from abroad. The U.S. Intelligence Community takes, as its charge, the need to monitor all corners of the globe all of the time. That is a real "mission impossible." The task would be even more unthinkable if analysts were solely, or even primarily, dependent on clandestinely acquired information with which to form judgments and deepen their knowledge. This is where open sources become invaluable, be they news sources, blog writers, academic contacts, informed observers, or others whose views and reportage are both credible and useful.[16] To know everything and to be constantly on top of every account, country, or issue, is not incumbent upon all-source

intelligence analysts, but rather to know who is, where the trustworthy sources are to be found, and how to make good use of them as the needs arise. While most people have abandoned their paper Rolodexes crammed with notes and business cards, the electronic equivalent is now the *sine qua non* in both intelligence and business.

Instant analysis by television's talking heads, the 24-hour news cycle, and competing purveyors of ideologically grounded and selected news and commentary now crowd the field and often seem to displace intelligence-based analysis and reporting. Decisionmakers and their spokespersons play catch-up with the news feeds, be they factual, biased, or simply bogus. Speedy coverage, instant commentary, and live video have overtaken seasoned expertise and thoughtful assessment. Nonetheless, these major sources of information competition for the intelligence world are now well-established and growing.

To establish the credibility of many open sources is extremely difficult. Those tasked with trying to exploit foreign news coverage and reportage must know where the sources of such reporting lie, the editorial and selection biases of news managers, and the relationship between news organs and those in power, both politically and economically. Published news is not intelligence and is not the intent or yield of collection. "It is the particular organization of the material for the decision maker that may turn publicly available news into intelligence."[17] Knowing the difference in, say Germany, between the tabloid *Bild Zeitung*'s orientation and that of the more intellectual *Die Zeit* is critical. The challenge is to know which news sources spout the government line and which routinely voice an opposition perspective.

Even that is easier to do than to rate the accuracy and utility of self-appointed news sources and commentators. "News" reporting is no longer the sole or privileged purview of trained (and preferably objective) journalists. But how and by whom are the credibility and utility of blogs rated? Some are insightful; many are trashy or vitriolic. Blogs are not static, and seldom do they have a reliability record that can be relied upon with confidence. That said, regardless of the veracity or logic of content, the size of a blog's receptive audience can be every bit as important as its messaging per se. That is why the users and follower numbers for Twitter and the like are tracked. Impact is as important as content, and sometimes more so. Journals, books, public speeches and interviews, policy pronouncements, propaganda, blogs, and tweets are in the public domain. Much in the news and the other sources can alert, inform, warn, and contextualize, as well as trigger and point to requirements for enhanced or new intelligence collection and coverage. And therein lies a true treasure trove of analytically useful open source information—if it can

be found within the masses of irrelevant, indeed often misleading, information. All of this plays into the issue of galloping, and often conflicting, OSINT.

… BUT BEWARE OF FOREIGNERS!

Although one of the best and most direct ways to acquire open source information about the world is to talk with foreigners, that approach remains largely a taboo in the U.S. Intelligence Community. Notwithstanding the inability and futility in attempting to track developments in every country on earth every day and hour—without open sources, a totally unimaginable task—the Intelligence Community remains in thrall to an overweening focus on secrecy and security. Too many of its personnel are caught in the risk avoidance web that considers all foreigners, including any contact with them, suspect. Because dealing with foreigners is deemed fraught with peril and personal vulnerabilities, it is best either avoided completely or left to a few, senior specialists. Anyone subject to a periodic polygraph examination in order to retain clearances and employment runs the risk of having questions about "foreign contacts" derail an otherwise routine exam.

Yet, analysts charged with monitoring and understanding foreign people and events are unlikely to do so as effectively if they lack access to informed or influential insights—social, cultural, economic, political, and otherwise—regarding those foreign countries and their leaders, parties, armies, perspectives, and narratives. How else, except through contact, can analysts keep some level of continuing attention on all parts of the globe, from Kenya to Korea to Kiribati? Open sources of information supply much of the raw material with which to build up, expand, and refine the general knowledge base. Occasionally, actual direct communication with foreigners, be they scholars, journalists, think tank analysts, blog writers, or, in some cases, government officials, makes a lot of sense, except perhaps to paranoid counterintelligence types. The key is to train all analysts to be attentive, discerning listeners when in the company of foreign "sources of information," volunteering little themselves, other than posing additional questions. With an enlightened use of open sources, such "risky" direct contacts can minimize security risks while enhancing analytic expertise.

OPEN SOURCE CHALLENGES

While many analysts lament the overwhelming amount of information they confront, in still too many notable instances, even in the open domain, insufficient information is available. That can be the result of a relative "Internet darkness," usually in those societies and states where the Internet's reach has not yet been fully felt or where governments have purposely moved

to block Internet access. Since the Internet and the social media that ride on it can be means to incite and coordinate protests, to convey opposition complaints and accusations, and to generate calls to action, regimes that abhor being challenged attempt to silence the net. Given the tendency of authoritarian regimes to try isolate their publics from outside news and connections, as did the Soviets during their years in power, can the Intelligence Community contribute to efforts to counteract such electronic blockades?

While the U.S. and its partners are ill-equipped to enforce Internet openness, "freedom of information," or "sunshine laws" in foreign states, one aim of U.S. foreign policy, and of the Department of State, is to foster an open Internet environment worldwide. Those efforts range from issues of advocacy of Internet access (a passive action) to actually enabling Internet rights (an active ability to facilitate usage of the Internet for communication and information). In other instances, governments and their surrogates use the Internet to distribute their own propaganda, as well as false and distorted accounts of events, and manipulated and deceptive information, making analysis perhaps more important but also more difficult. In the most extreme cases, the issue is not distortion but actual denial of service. Estonia experienced this from Russia in April 2007 after removing a Soviet-installed monument from the center of Tallinn, the capital.[18]

Another flaw in the exploitation of open sources has to do with published strategies, intentions, and visions. Too often published opinion is dangerously ignored or overlooked. Many a leader has telegraphed his/her beliefs and intentions. Had the world read and taken heed of Adolf Hitler's *Mein Kampf* or made more of Osama bin Laden's stated strategy of forcing the West to spend itself into oblivion to pay for counter-terrorism and security protection, some terrible historic events might have been either averted or diminished.[19] Those malevolent intentions had been both telegraphed and openly accessible, even if largely discounted.

DENIAL VS. DECEPTION: CREDIBILITY IN THE ERA OF "FAKE NEWS"

To be sure, some allegedly open source information conduits, like the dark web, are not so easily penetrated, at least not overtly. But when assessing the truthfulness and utility of open source information, denial is less the issue than is deception. Any computer user or Internet visitor knows full well the range of scams, phishing, ransomware, and other schemes intended to deceive and defraud the public. The Intelligence Community must today determine whether its increasing focus and reliance on (as well as concern over) open source information still fulfills the necessary all-source intelligence function. Source validation is every bit an OSINT requirement and priority. Gathering and protecting the information that others consciously try to deny or conceal

is a huge challenge that must be met, especially if the intelligence collection and analysis performed by government agencies is to be more precise, relevant, and timely than that provided by commercial or journalistic entities. In the area of OSINT, however, the general thrust is often the marketing of a point of view, ideology, bias, belief, or product, regardless of its value or truth.

The U.S. Intelligence Community must offer, now and in the future, a quality of information that Stratfor, Oxford Analytica, Economist Intelligence, CNN, Fox News, *The New York Times, Wikipedia,* Google, and others cannot and do not provide, regardless of their quality and opinion slant. This area needs and deserves a completely separate treatment. But the solution lies, in part, in those specialized intelligence arenas exclusive of "open source intelligence," of which all of the IC's clandestine INTs are a part. In fact, those secretly acquired bits of information and perspectives can and often do serve the purpose of either validating or discrediting public information, initial reporting, and instant interpretations. Note how often instant, published reactions to an event or a decision have been proved wrong. This area remains under-developed in the fact-checking enterprise, although some efforts have been made in assessing its accuracy.

OSINT: INFORMATION SERVING AN INTELLIGENCE PURPOSE

Open source information is not and does not become intelligence until or unless it fills an intelligence gap or need. This caveat applies overall to intelligence collection, mining public as well as very private realms, and to the yield's inclusion in or inspiration for all-source intelligence analysis.[20] Non-OSINT intelligence achieves status at the point of collection, while OSINT acquires it only if and when it is applied in an intelligence role. In light of both globalization and brisk advances in technology and worldwide telecommunications, the wealth of information afloat in today's world is astonishing when compared to earlier, not too distant, decades when access to denied areas or information required clandestine means and tradecraft. Hiding information, regarding both capabilities and intentions, was traditionally a fundamental part of realist statecraft and, by the same token, seeking to uncover it was the essential *raison d'etre* of intrusive, clandestine intelligence operations.

Unchanged, however, is the kind of information that demands protection once it has become intelligence or is drawn upon for intelligence analysis. Interestingly, that aspect applies regardless of whether the information was openly obtained or clandestinely collected. Thus, an intelligence analysis of, say, the presumed motivations of a foreign leader—drawing on no clandestinely-acquired information or secret insights—can be and still is protected intelligence for the end-user. If it is to be and remain valuable, it

requires non-disclosure except to those with an authorized need for it, lest it become known to the subject of the assessment. What is said about or to others in public is open and free; what analysts say about others to decisionmakers is not. The confidential, intelligence-informed judgments that analysts share with their consumers are no one else's business.

Michael Warner has noted that any definition of intelligence must include "a consideration of secrecy, … [the potential that it could] mean life or death, … [and] both clandestine activity as well as information."[21] Indeed, the word "intelligence" in modern usage has taken on a semantic meaning connoting confidentiality, if not espionage, at least in the United States, France, Russia, and Germany.[22] That negative connotation of the word "intelligence" has long prompted the United Nations (UN) to strenuously avoid its use. Collecting furtively against fellow UN member states is deemed a major taboo. Likewise, the Japanese have had an aversion to calling some things intelligence. For years, Japanese officials have labeled their array of intelligence satellites "information gatherers."[23] Yet, what, if anything, about OSINT needs to be concealed? For foreign government analysts and "collectors," one caution is the fact that information intended for one audience, their own, might be exploited by another, namely, the U.S. Intelligence Community. For example, the study by outsiders of published Chinese research endeavors that are posted in that country's professional and scholarly journals offers a case in point. Any apparent U.S. official interest in a foreign information source, by agencies or individuals using government computers for the on-line inquiry, can prove detrimental. Suddenly, what once appeared in the public space goes dark.

PRIVACY VS. SECRECY IN THE CONTEXT OF "OSINT"

The uninitiated have difficulty fathoming why an analysis based solely on open source/public domain information can still end up being classified. But analysts' judgments, regardless of their motivating evidence, are no one's business outside the circle of approved access, until or unless a conscious decision is taken to make them public. Pre-clearance procedures for publishing and speaking publicly by intelligence personnel have their purpose and import. What U.S. intelligence analysts are telling their colleagues or government officials about a foreign country's leader, intentions, or perspectives is not for the subject of that assessment to know or learn. Herein lies the essence of the problem of leaks. Leakers knowingly violate their employment oaths[24] and national security procedures, notwithstanding their purported ethical aims or motivation. That is a primary reason why intelligence as processed information is generally kept secret, just as most private sector companies fervently protect their unique proprietary information.

Among the most closely held secrets in the United States are not only the launch code for nuclear missiles but also the formula for the syrup used in making Coca Cola. That formula is stored in a Fort Knox–style vault at corporate headquarters in Atlanta, Georgia, to be accessed by only those few with a validated "need to know." To underscore the example, some years back two Coke employees with such purported access offered to sell the syrup formula to the competitor, Pepsi Cola, for millions of dollars. Pepsi reported their treacherous offer to police, who then ran a sting operation. Subsequently tried and convicted of a felony theft attempt,[25] the pair were sentenced to five- and eight-year federal prison terms.[26] This was clearly a case of attempted industrial espionage, reminiscent of convictions for national security violations in espionage or leak cases. And Coke's "secret formula" is still secret.

Since at least 2014, the U.S. National Security Agency (NSA) has been under intense scrutiny and pressure concerning its reported collection and retention of e-mails and other correspondence generated by and for U.S. persons. Much of that turmoil was the result of claims by whistleblower Edward Snowden, a one-time NSA contractor. Rumors abounded that the NSA was vacuuming up every e-mail sent and storing it for analysis and retention, perhaps at its mammoth data center in Utah.[27] While such extreme government collection was routinely denied and never validated, it illustrated another complicating, ethical aspect of dealing with open source information. Acquiring gray literature, from newsletters to blogs to underground publications, is one thing. Scooping up private correspondence and snooping upon Americans is, of course, quite another matter, and U.S. and publics elsewhere were upset by such allegations of NSA excess.

Two related issues involving open sources are their occasional nefarious use and the justified concern over the erosion of privacy in this Internet age. Groups of all kinds engage in unlawful, often violent activities; they also use the Internet to recruit, train, motivate, communicate, and propagandize. Those actions are of keen interest to the Intelligence Community in serving national security, law enforcement, and public safety. Moreover, the Internet, World Wide Web, and an ever-expanding array of social media, from Facebook and Instagram to Linked.in and others, are channels of information that afford little (and, in some cases, no) protection from peering eyes, hackers, and malicious actors.

The public's trust in privacy protection is now thin and rightly so. As Amanda Hess noted in a *New York Times Magazine* article, "Our 'privacy' has become a key currency in online life—traded away in return for convenient services and cheap thrills. … It is increasingly seen not as a right but as a luxury good. … Data-mining companies know everything about us, but we know very little about what they know."[28] "Friending" on Facebook is a supposedly protected activity, if users set their privacy protections

properly, but "tweeting" to the world, even if done by the President of the United States, is not. Moreover, the prevalence of "fake news," deceptive schemes and scams, spam e-mails, spear-phishing efforts, "monetizing" users' information and purchase trends, and other obscured and and/or malevolent actions make the sorting of good data from the huge volume of useless garbage found in open sources a demanding, if not often impossible, task.

SO, IS OSINT INTELLIGENCE?

Something calling itself OSINT has become an integral part of all-source intelligence, both in its acquisition and usage. The IC would be increasingly hamstrung, if not blind, without it. But the challenges in OSINT's acquisition and usage differ from those of the clandestine collection disciplines and their major U.S. three-letter agency managers. They require the seekers to determine which sources of information, most of which are out there in the open and free for the taking, afford analysts what they need in order to make sense of foreign decisions, perspectives, and likely developments for the benefit of end-users.

The answer to the question as to whether open source information belongs in the family of the clandestine collection approaches remains shaded toward the negative. OSINT is not classified at the point of collection. It is simply viewed or, if necessary, purchased. It need not be purloined, even if it is shielded upon taking on an intelligence role. Indeed, open source information found not useful can be simply discarded into a circular file, whereas clandestine collection products still require disposal in a shredder or burn bag.

Coining a unique acronym, OSINF (for information *vice* intelligence), while perhaps more accurate, remains an unmarketable and tardy compromise. Suffice it to say that open source information's potential for intelligence use is undeniable, even if its definition as another, stand-alone intelligence discipline—and one even perhaps deserving a separate agency—is less than convincing.

REFERENCES

[1] See John C. Gannon, "The Strategic Use of Open-Source Information," *Studies in Intelligence*, Vol 45, No. 3, 2001, p. 67.

[2] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 4th ed. (Washington, DC: CQ Press, 2009), p. 1. In this context, recall that in the practices of the United Nations, there is a profound inclination to shun "intelligence" by that name (implying the UN condoning spying among member states) in favor of the more anodyne "information."

[3] Mark M. Lowenthal, "Open-Source Intelligence: New Myths, New Realities," in *Intelligence and the National Security Strategist: Enduring Issues and*

Challenges, Roger Z. George and Robert D. Kline, eds. (Washington, DC: National Defense University Press, 2004), pp. 273–278.

[4] Thomas Fingar, *Reducing Uncertainty: Intelligence Analysis and National Security* (Stanford, CA: Stanford University Press, 2011), p. 6.

[5] The reference to Sims as originator stems from a lecture given in March 2017 by Mark Lowenthal.

[6] Jennifer Sims, "What is Intelligence? Information for Decision Makers," in *U.S. Intelligence at the Crossroads: Agenda for Reform*, Roy Godson, Ernest R. May, and Gary Schmitt, eds. (Washington, DC: Brassey's, 1995), p. 4.

[7] Open Source Collection Officer—Central Intelligence Agency, available at https://www.cia.gov/careers/opportunities/analytical/open-source-officer-foreign-media-an, accessed 17 May 2017.

[8] See https://www.cia.gov/careers/opportunities/analytical/open-source-officer-foreign-media-an, accessed 23 May 2017.

[9] For one strong view on the need for a separate OSINT agency, see Mark Lowenthal, "Open-Source Intelligence," pp. 273–278.

[10] *U.S. National Intelligence: An Overview*, Intelligence Community Information Sharing Executive, 2013, p. 46.

[11] This coinage comes from Lt. Colonel Jennifer Smith-Heys, a member of the National Intelligence University graduate faculty.

[12] Eliot A. Jardines, "Open Source Intelligence," in *The 5 Disciplines of Intelligence Collection*, Mark M. Lowenthal and Robert M. Clark, eds. (Washington, DC: CQ Press, 2016), pp. 6–7. Jardines's is among the most comprehensive and historical treatments of open source information/intelligence. For a recent exultation of the value of open sources, see James M. Davitch, "Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data," *Joint Forces Quarterly,* No. 87, 1 October 2017.

[13] Ernest R. May, "The Twenty-First Century Challenge for U.S. Intelligence," in *Transforming U.S. Intelligence*, Jennifer E. Sims and Burton Gerber, eds. (Washington, DC: Georgetown University Press, 2005), p. 8.

[14] Although perhaps apochryphal, former CIA Director Allen Dulles, foremost a collector, reputedly defined an analyst as "a person who takes 49 documents and creates a 50th."

[15] My observation is based on 50 years in the business of U.S. all-source intelligence analysis at the national level in more than one agency.

[16] See also Bowman H. Miller, "Improving All-Source Intelligence Analysis: Elevate Knowledge in the Equation," *International Journal of Intelligence and CounterIntelligence*, Vol. 21, No. 2, Summer 2008, pp. 337–354.

[17] Jennifer Sims, "What is Intelligence?," p. 5.

[18] "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, available at http://www.iar-gwu.org/node/65, accessed 12 July 2017.

[19] In this context, recall the fateful claim made by George C. Scott, playing the motion picture role of General George Patton when he confronted the Desert

Fox, German General Erwin Rommel, with the assertion: "I read your damn book!"

[20] It is useful to note that, unlike U.S. intelligence, British intelligence—particularly foreign intelligence—remains resistant to incorporating much, if any, open source information in its multi-agency assessments.

[21] Michael Warner, Comments re "What is Intelligence Theory?" in *Toward a Theory of Intelligence: Workshop Report* (Conference Proceedings), Gregory F. Treverton et al., eds. (Santa Monica, CA: The RAND Corporation, 2006), pp. 2–3.

[22] *Ibid.*

[23] In January 2017 Japan launched the "twelfth member of the Information Gathering Satellite (IGS) series of optical and radar observation platforms … ," "Japan pursues military satellite deployment," available at http://www.aircosmosinternational.com/japan-pursues-military-satellite-deployment-91901, accessed 21 March 2017. *Mainichi* headlined: "Japan Successfully Launches Intelligence-Gathering Satellite," available at http://mainichi.jp/english/articles/200170317/p2g/00m/0dm/069000c, accessed 17 March 2017.

[24] For reasons quite unclear to me, Intelligence Community contract personnel are not required to swear the oath to protect and defend the U.S. Constitution.

[25] Author visit to Coca Cola Headquarters, Atlanta, March 1996.

[26] "Two Ex-Coke Workers Sentenced in Pepsi Plot Deal," *CNN* on-line, 23 May 2007.

[27] "NSA Utah Data Center," *Facilities Magazine*, 14 September 2011, available at http://facilitiesmagazine.com/utah/buildings/nsa-utah-data-center, accessed 24 April 2013, and https://www.theblaze.com/stories/2013/07/01/seven-stats-to-know-about-nsas-utah-data-center-as-it-nears-completion, accessed 4 October 2017.

[28] Amanda Hess, "Open Secrets," *The New York Times Magazine*, 14 May 2017, pp. 11, 13.