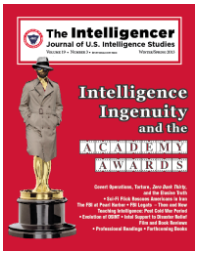

From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 19 • NUMBER 3 • $15 SINGLE COPY PRICE Winter/Spring 2013 ©2012, AFIO

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE STE 324
FALLS CHURCH, VA 22043
Web: **www.afio.com**, E-mail: **afio@afio.com**

Guide to the Study of Intelligence

The Evolution of Open Source Intelligence (OSINT)

by Florian Schaurer and Jan Störger

This article presents the views on open source intelligence by two European authors and practitioners.

Introduction

Here, the term OSINT is defined as the collection, processing, analysis, production, classification, and dissemination of information derived from sources and by means openly available to and legally accessible and employable by the public in response to official national security requirements. This article addresses the genesis of OSINT as an intelligence discipline, arguing that it should rather be referred to as tradecraft, as well as its contributions to an integrated, all source knowledge management process within the intelligence enterprise.

History of OSINT

The history of exploiting open information reaches back to the emergence of intelligence as an instrument supporting a government's decisions and actions. Yet, it was not a methodical effort until the United States pioneered the institutionalization and professionalization of a stand-alone capacity for monitoring foreign media, with the establishment of the Foreign Broadcast Monitoring Service (FBMS), which grew out of a research initiative at Princeton University. The FBMS rapidly gained momentum after the Japanese attack on Pearl Harbor. In 1947 it was renamed the Foreign Broadcast Intelligence Service (FBIS) and put under the newly established CIA. In 2005, following the attacks of 9/11 and the passage of the Intelligence Reform and Terrorism Prevention Act, FBIS – with other research elements – was transformed into the Director of National Intelligence's Open Source Center (OSC). Since its establishment, the OSINT effort has been responsible for filtering, transcribing, translating (thus interpreting) and archiving news items and information from all types of foreign media sources.

In 1939, the British government asked the British Broadcasting Corporation (BBC) to launch a civilian, and later commercial, service scrutinizing foreign print journalism and radio broadcasting with its Digest of Foreign Broadcasts, later entitled the Summary of World Broadcasts (SWB) and now known as BBC Monitoring. As a BBC handbook from 1940 has it, the aim was to erect a "modern Tower of Babel, where, with exemplary concentration, they listen to the voices of friend and foe alike." By mid-1943 the BBC monitored 1.25 million broadcast words daily. A formal partnership between the BBC and its US counterpart was instituted in 1947/48 with agreement on the full exchange of output. Also in 1948, the research arm of the US Library of Congress was established out of the Aeronautical Research Unit to provide customized research and analytical services using the vast holdings of the library. It is now known as the Federal Research Division (FRD).

During the Cold War, countries on both sides of the Iron Curtain created open source collection capacities, often embedded in their clandestine intelligence services. Open sources not only "constituted a major part of all intelligence," according to CIA analyst Stephen Mercado, but eventually became "the leading source" of information about the adversaries' military capabilities and political intentions, including early warning and threat forecasting. For example, the East German Ministry for State Security (MfS, known as the "Stasi") analyzed 1,000 Western magazines and 100 books a month, while also summarizing more than 100 newspapers and 12 hours of West German radio and TV broadcasting daily.

Open sources during the Cold War were already a well-established resource of information, often the first resort for targeting other collection efforts, or "the outer pieces of the jigsaw puzzle," as Joseph Nye put it.[1] With Internet technology, publicly available information has had a tremendous impact on every aspect of modern-day political, social, and economic life. One needs to be aware, though, that the Internet itself is not a source (except for its meta data); rather it is a means to transport information and a virtual location.

Most intelligence communities were slow in appreciating the value of the Internet for two reasons: (1) Intelligence agencies seek an informational advan-

1. Committee on Homeland Security: Giving a Voice to Open Source Stakeholders. (2008) *http://chsdemocrats.house.gov/SiteDocuments/OpenSourceReport.pdf.*

tage through covertly dealing with secrets. Relying on open information and its respective copyright restrictions runs counter to that idea. (2) In most cases it is more difficult, risky and expensive to apply clandestine methods in order to acquire secret sources, thus giving the impression that those sources must be of higher value than open sources, confusing the method with the product or mistaking secrecy for knowledge.

After the collapse of the Soviet Union, Western intelligence agencies redirected their operations to new geographic and thematic priorities, such as Africa and Asia, non-state actors, low intensity conflict in expeditionary environments, political and religious terrorism, the proliferation of weapons of mass destruction (WMD) and the vulnerabilities of computer networks, which resulted in a greater emphasis on open sources. The US military first coined the term OSINT in the late 1980s, arguing that a reform of intelligence was necessary to cope with the dynamic nature of informational requirements, especially at the tactical level on the battlefield. In 1992, the Intelligence Reorganization Act defined the objectives of information gathering as "providing timely, objective intelligence, free of bias, based upon all sources available to the US Intelligence Community, public and non-public." In 1994, the Community Open Source Program Office (COSPO) was established within the CIA. In 1996, the Commission on the Roles and Capabilities of the US Intelligence Community (more commonly known as the Aspin-Brown Commission) concluded "a greater effort also should be made to harness the vast universe of information now available from open sources." Parallel efforts by NATO to generate a framework for the use of OSINT led to the publication of several handbooks, primers and practical manuals of varying quality. With the European Media Monitor (EMM) and an OSINT Suite, among other tools and projects, the European Union (EU) Commission's Joint Research Centre (JRC), is developing its own instruments for tackling the challenges that the ever-growing flood of information poses.

9/11 proved to be a watershed for OSINT, with the National Commission on Terrorist Attacks upon the United States (9/11 Commission) in 2004 recommending the creation of an Open Source Agency without further comment or detail. This concept was picked up in 2005 – along with respective recommendations by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) – when the Director of National Intelligence (DNI) established the OSC, absorbing the CIA's FBIS with the World News Connection (WNC) under the supervision of the National Technical Information Service (NTIS). The OSC presents itself as the "US Government's premier provider of foreign open source intelligence [and] provides information on foreign political, military, economic, and technical issues beyond the usual media from an ever expanding universe of open sources." At the same time, an Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS) was appointed, increasing the visibility of the National Open Source Enterprise. With the development of regional fusion centers, which are focused on homeland security and law enforcement issues, OSINT is a major source in merging and consolidating relevant intelligence into actionable products.

OSINT and the Private Sector

In economic terms, national security as a public good is provided efficiently only by the government or under state supervision. Despite its substantial value OSINT requires no special permissions. Because non-state contractors may be superior regarding their capabilities and resources for delivering OSINT, they can contribute to a better provision of national security. Intelligence derived from sources or using means that are openly available, but illegal, should not be considered OSINT, e.g. leaks of classified information, the legal status of which is in question, or proprietary information. CIA's venture capital firm In-Q-Tel's investment in Recorded Future, a web-monitoring predictive analysis tool, proves former CIA director Michael Hayden's statement that "secret information isn't always the brass ring in our profession."[2]

A crucial point in government-private sector partnerships for OSINT is the need for non-disclosure regulations to protect national security. Sometimes, an intelligence product based solely on openly available information must be classified to protect the government's interest from being revealed. Intelligence agencies must integrate and control outreach activities and contractors' efforts to prevent jeopardizing operational and national security. Partnerships with academia avoid potential conflicts between the state and profit-oriented players. Universities are a fertile ground for capturing expertise that exists within the public sphere and can be ideal partners for intelligence agencies.

The fact that open sources often provide the

2. Noah Shachtman: Google, CIA Invest in 'Future' of Web Monitoring. (2010) *http://www.wired.com/dangerroom/2010/07/exclusive-google-cia/*.

majority of intelligence input makes OSINT an essential part of an all-source intelligence effort. Every intelligence professional should be knowledgeable of OSINT sources and methods, especially as analysis and collection are increasingly merging with each other. Nevertheless, outreach activities and open source exploitation have to be supported by specialized elements to ensure that analysts keep up with emerging technologies and the market. Specialized OSINT experts are most qualified to identify potential capability gaps and to assess where contractors can be of use. One good way to integrate the knowledge and skills of the private sector into the Intelligence Community is an OSINT certification program, currently being introduced in the US, for example.

Challenges facing OSINT

Because of its open nature, OSINT can facilitate sharing. But the means for sharing need to be improved for OSINT as well as for more restrictive categories of intelligence. This need exists not only in the national security community, but also with those charged with domestic security and enforcement of laws. Thus, a vertically and horizontally consistent sharing and safeguarding system must be established.

Openness is important for governments' credibility and justifying their decisions to the public and international allies. However, there is an inherent vulnerability if an adversary uses open sources to undermine the state's national security. OSINT can be used for vulnerability evaluations of one's own nation.

Adversarial states will also manipulate open sources for deceptive purposes. However, in today's world, with vast amounts of information openly available, such deceptive schemes become more difficult.

Although the fast pace of developing information technology is an important challenge, the human factor should not be underestimated. Ultimately, it is always human expertise that makes the difference in intelligence tradecraft. Collectors and analysts therefore need both legal and practical training, the appropriate literacy, and first-class technical capabilities (such as data mining, network analysis and translation solutions) to put disparate pieces of raw OSINT data into context and make sense of them. With the advent of new Internet-based media, the variety, volume and velocity of information multiply. Today's challenge is no longer "connecting the dots," but organizing the information flow, distinguishing between signals and noise, and by validating sources in a timely manner to support both government decision makers and the war fighter.

READINGS FOR INSTRUCTORS

An excellent overview of the Open Source Center's policies, procedures, and products is in Hamilton Bean, "The DNI's Open Source Center - An Organizational Communication Perspective" in *International Journal of Intelligence and Counter-Intelligence*, Volume 20, Issue 2 (2007).

Magdalena Adriana Duvenage, a South African scholar, provides a solid examination of the impact of the information revolution on intelligence analysis and knowledge management in *Intelligence Analysis in the Knowledge Age* (2010), available at *http://scholar.sun.ac.za/bitstream/handle/10019.1/3087/Duvenage,%20M.A.pdf?sequence=1*.

Stevyn Gibson, in his 2004 publication "Open Source Intelligence - An Intelligence Lifeline" gives a brief synopsis of the emerging role of OSINT, drawing together the contextual influences that are bringing about its potentially starring role. Available at *http://www.rusi.org/downloads/assets/JA00365.pdf*.

Arthur S. Hulnick, a professor at Boston University and former CIA officer, has written "The Dilemma of Open Source Intelligence - Is OSINT really intelligence?" in Loch K. Johnson, editor, (2010) *The Oxford Handbook of National Security Intelligence*. This is a scholarly article on the role of OSINT in and for the private sector, OSINT and intelligence reform, and the counter-intelligence aspects of OSINT.

William J. Lahneman's 2010 article, "The Need for a New Intelligence Paradigm," in the *International Journal of Intelligence and Counter-Intelligence*, Volume 23, Issue 2, is an important text on the IC's organizational culture that emphasize secrecy, not knowledge sharing, arguing that facilitating both kinds of information flows require a new approach to the intelligence enterprise.

An insightful public discussion about the government's practical needs for OSINT is the LexisNexis "Open Source Intelligence Roundtable: OSINT 2020 - The Future of Open Source Intelligence," available at *http://www.dni.gov/speeches/Speech_OSINT_Roundtable_20100617.pdf*.

Other reference items related to OSINT include the following. Harris Minas: "Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?" (2010), at *http://rieas.gr/images/rieas139.pdf*. This is an academic thesis addressing OSINT as an issue of research for critical intelligence studies.

NATO (2001), *Open Source Intelligence Handbook*. Available at *http://blogs.ethz.ch/osint/files/2010/08/nato-osint-handbook-v12-jan-2002.pdf* This is a rather outdated guidance for NATO staff on open source exploitation with the Internet being the default C4I architecture, arguing that a robust OSINT capability enables intelligence staffs to address

many intelligence needs with internal resources.

Brian Rotheray, (2009), *A History of BBC Monitoring*. *http://www.monitor.bbc.co.uk/about_us/BBCMhistory%20revisions%20x.pdf*. This book celebrates the first 70 years of BBC Monitoring and covers the main political, technological and social aspects of its history.

Stephen C. Mercado, (2004), "Sailing the Sea of OSINT in the Information Age," *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html*. This is a classical account of OSINT expanding into the areas of HUMINT, IMINT, and SIGINT, thereby demanding a sustained approach by the IC to open sources.

These several directives directly or indirectly address OSINT policies and applications. United States Department of the Army: *Open Source Intelligence* FMI 2-22.9. (2008). Available at *http://ftp.fas.org/irp/doddir/army/fmi2-22-9.pdf*. This is the US Army's interim doctrine, serving as a catalyst for analysis and development of OSINT training, concepts, materiel, and force structure.

United States Department of Defense Instruction No. 3115.12: *Open Source Intelligence*. (2010) *http://www.dtic.mil/whs/directives/corres/pdf/311512p.pdf*. This directive establishes policy, assigns responsibilities, and prescribes procedures for OSINT operations within the US Department of Defense.

United States Intelligence Community Directives No. 301 (2006), No. 205 (2008), No. 304 (2008), No. 623 (2008), No. 612 (2009). Available at *http://www.fas.org/irp/dni/icd/*.

United States Open Source Center (OSC): *History*. (2009) *https://www.opensource.gov/public/content/login/attachments/202244099/255164545.pdf*. This is a one-page history of OSC.

Kurt Werren, Kian Fartab, (2010), *All Source Collection* – Kernstück eines leistungsfähigen Nachrichtendienstes. Available at *http://www.asmz.ch/fileadmin/asmz/ASMZ_aktuell/2010_04/All_Sources_Collection_Deutsch_1_.pdf*. This is an important contribution to the improvement of all source collection, analysis and production (in German).

Florian Schaurer works as a political scientist for the German Armed Forces. He holds a PhD in political philosophy from the University of Zurich, a Master's degree in political science, philosophy and religious studies from the University of Heidelberg, and a Master's in human rights law from the University of Oxford.

Jan Störger is an information security expert. He holds master level degrees from the University of Mannheim (Dept. of Economics) and the Panthéon-Sorbonne University in Paris (Dept. of Law).