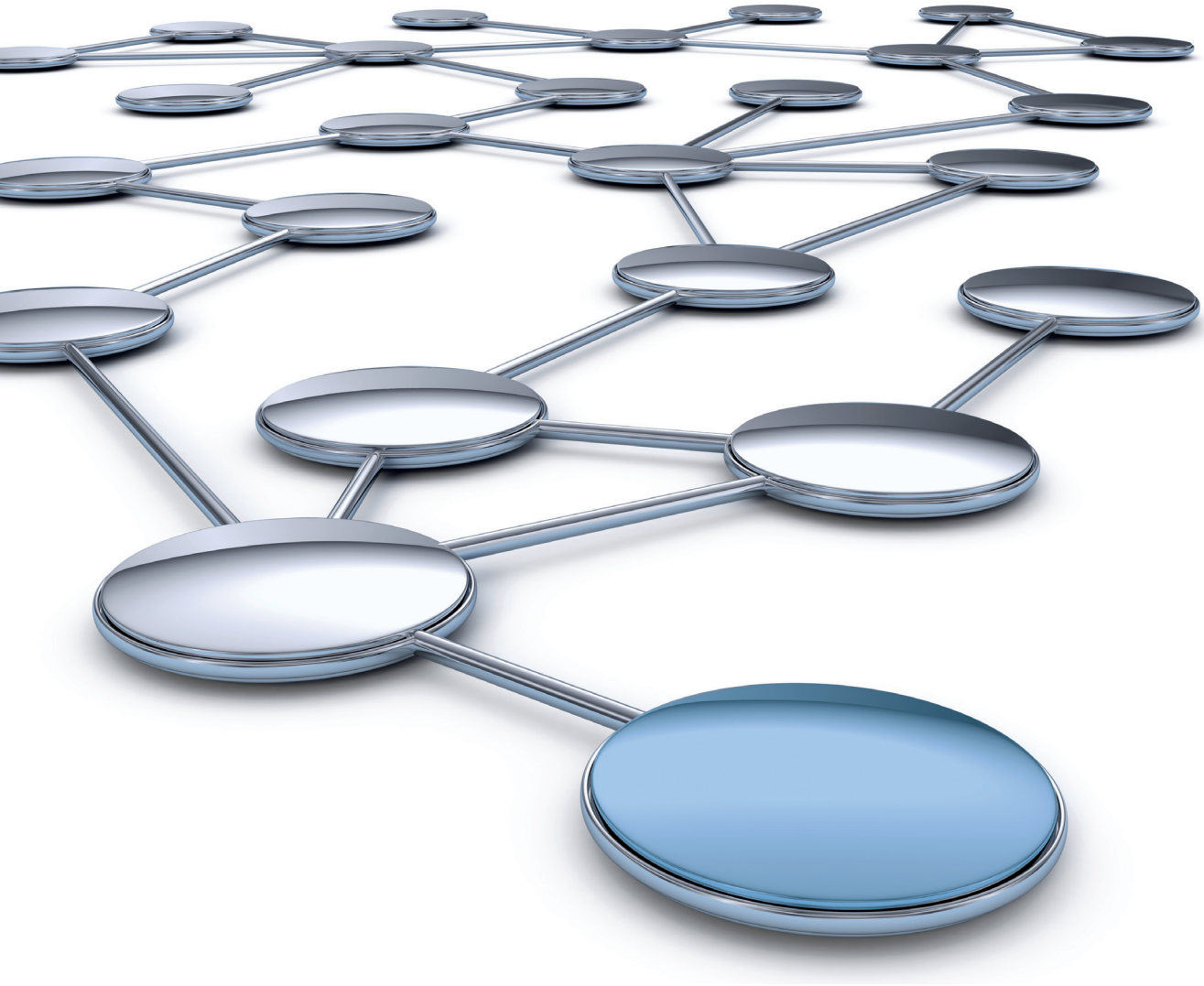

OSINT

Report 3/2010

ISN ETH Zurich

INTERNATIONAL RELATIONS AND SECURITY NETWORK

ETH Zurich | Leonhardshalde 21, LEH | 8092 Zurich | Switzerland
Tel: +41 (0)44 632 04 24 | Fax: +41 (0)44 632 14 13
www.isn.ethz.ch | osint@sipo.gess.ethz.ch

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Authors: Florian Schaurer, Jan Störger

International Relations and Security Network (ISN)
ETH Zurich
Leonhardshalde 21, LEH
8092 Zurich
Switzerland
Tel.: +41 (0)44 632 04 24

osint@sipo.gess.ethz.ch
www.isn.ethz.ch

Project supervision: Andreas Wenger, Director CSS; Victor Mauer, Deputy Director CSS

OSINT Report 3/2010

The Evolution of Open Source Intelligence

Introduction

This report provides a brief panorama of the development, role and challenges of *Open Source Intelligence (OSINT)* in today's *Intelligence Communities (ICs)*. It addresses both the genesis of OSINT as a so-called *intelligence discipline*, arguing that it, primarily, should refer to actual *tradecraft*, as well as its potential contributions to an integrated *all source* knowledge management and information-sharing effort within the intelligence enterprise.

Definition

In the following, the term OSINT is understood as the systematic collection, processing, analysis and production, classification and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security.

History

The history of more or less methodically exploiting openly available and legally accessible information reaches back to the very emergence of intelligence as an instrument for gathering relevant information to support a government's decisions and actions with regards to national security and defense. Namely in media monitoring, which in its early stages meant pure newspaper clipping, the commercial sector has long been ahead of governmental efforts. Not before the professionalization and formal institutionalization of intelligence as an indispensable component of a national (and later, where applicable, transnational) security apparatus in the second half of the twentieth century has the governmental collection and analysis of open sources evolved from common, though hardly structured, practice into a distinct domain of strategic importance, requiring its own set of tools and rules. Until today, the history of OSINT to a large extent is an American history.

The United States pioneered the buildup and further development of a stand-alone capacity for monitoring, filtering, transcribing, translating (thus already interpreting) and archiving news items and information from foreign media sources with the establishment of the *Foreign Broadcast Monitoring Service (FBMS)* in 1941, succeeding a respective research initiative at Princeton University. The FBMS which, in 1947, was renamed the *Foreign Broadcast Intelligence Service (FBIS)* and put under CIA supervision until it was transformed into the *Open Source Center (OSC)* in 2005, rapidly gained momentum after the devastating Japanese attack on Pearl Harbor, which is remembered as the single greatest failure of US secret intelligence until the cataclysmic terrorist attacks on September 11th, 2001.

Even prior to that, in 1939, the British government asked the BBC to launch a similar, yet civilian, and, later, commercial service scrutinizing foreign print journalism and the ever increasingly important radio broadcasting with its *Digest of Foreign Broadcasts*, later known as 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". A formal partnership between the BBC and its US counterpart came into being in 1947/48 with agreement on the full exchange of output and shared coverage based on avoiding duplication. Also in 1948, the *Federal Research Division (FRS)* was founded to provide "customized research and analytical services" using the vast holdings of the world's largest library, the US Library of Congress.

During the Cold War, other countries on both sides of the Iron Curtain were to follow with the creation of mainly subsidiary open source collection capacities, embedded in their clandestine intelligence environments, and soon 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 notorious East German *Ministry for State Security (MfS)* analyzed some

NOTES

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 each and every day.

Going hand in hand with this institutional progress and increasingly automated processing were massive advances in information and communication technology, namely the steadily growing usage of television, little by little attenuating the importance of radio as the primary openly available means for accessing ephemeral information besides the less time-critical printed material, which by then, much more so than in the modest beginnings of straightforward mass media monitoring, also comprised commercial databases, libraries, journals, conference proceedings, academic and *grey literature* and non-print material, e.g. audio-visual data.

It is fair to note that open sources during the Cold War were a very well-established resource of information, often even a first resort for targeting other collection efforts, or "the outer pieces of the jigsaw puzzle", as Joseph Nye put it. Yet the intelligence community continued to be very hesitant in appreciating their actual value for two reasons: 1. Intelligence agencies seek an informational advantage through covertly dealing with secrets; relying on open information runs counter to that idea. 2. In most cases it is more difficult, risky and more expensive to apply clandestine methods to acquire secret sources, thus giving the impression that those sources must be of higher value, apparently confusing the method with the product or mistaking secrecy for intelligence. Notwithstanding this insistent, de facto mainly semantic dismissal of open sources as genuine intelligence craft, the end of the Cold War has not least marked the triumph of open over closed regimes, demonstrating that no monopoly on information can be sustainable with ubiquitous sources of information floating in the ether.

Since what has subsequently been attributed the *information revolution* leading to an *information society*, with the internet being the most monolithic game changer in the 1990s, the technological, social and economic role of information has had a tremendous and undisputed impact on every aspect of life. More than ever before, the value of information as a factor of production and as a product itself becomes a focal point of scientific debate, distinguishing information from data, knowledge and wisdom. While information as organized data is furthermore considered the basis of knowledge, wisdom is understood as sound judgment built on solid knowledge, meaning that only data and information can easily be shared and transferred, whereas knowledge and wisdom depend on experience and expertise. In short: information, even plenty of it, without processing, analysis and production, classification and dissemination is not authoritative intelligence, now less than ever.

After the collapse of the Soviet Union, Western intelligence agencies were forced to redirect their operations towards 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 WMD and the vulnerabilities of vital computer networks. US military reconnaissance first coined the term *OSINT* in the late 1980s, arguing that a fundamental structural reform of intelligence is necessary to cope with the ever more dynamic nature of informational requirements and channels, be it tactically on the battlefield or strategically in the political arena. In 1992, the *Intelligence Reorganization* Act defined the objectives of any information-gathering program as "providing timely, objective intelligence, free of bias, based upon all sources available to the US Intelligence Community, public and non-public". Again, in 1996, the *Commission on the Roles and Capabilities of the US Intelligence Community* (more commonly known as the *Aspin-Brown Commission*) concluded that "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 within its realm have led to the publication of several handbooks, primers and practical manuals of varying quality on the subject between 2001 and 2002. With the *European Media Monitor (EMM)* and an *OSINT Suite* - among other tools and projects -, the EU *Commission's Joint Research Centre (JRC)*, meanwhile, is developing its own instruments for tackling the challenges that open sources pose to not only intelligence but information logistics and to keep pace with the ever-growing competition with private companies like *NewsTin*, *Cision* and *TNS*. It is mainly academia and private businesses that are spearheading innovations, such as real-life tone and sentiment detection, non-text pattern recognition, medical

NOTES

intelligence and forecasting applications, and which advance new thinking on internet surveillance and forensics.

9/11 proved to be a watershed, with the *National Commission on Terrorist Attacks Upon the United States* subsequently, in 2004, recommending the creation of an *Open Source Agency* without further comment or detail. This was picked up in 2005 – along with respective recommendations by the US WMD Commission – when the *Director of National Intelligence (DNI)* established the *Open Source Center*, absorbing the CIA's FBIS with the *World News Connection (WNC)* under the supervision of the *National Technical Information Service (NTIS)*. The OSC understands 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, noticeably strengthening the visibility of the whole *National Open Source Enterprise*, which not least profits from the increased build-up of regional *fusion centers* merging and consolidating all relevant sources into actionable products. The following national *Information Sharing Environment Initiative* and, finally, a common working definition of OSINT by the US supplied in 2006 with its *Congress Defense Authorization* Act mark the road ahead for further capacity development. The future intelligence professional is expected not just to be a guardian of information (potentially biased through the practice of *need-to-know*), but also a responsible trader thereof *(need-to-share)*.

Intermediate Findings

Some characteristic practical features of OSINT can be deduced from this retrospective of the systematic harvesting of information and the regular exchange thereof:

1. The press, public and published opinion, and the various media, corporate, academic and private channels account for a significant amount of openly available and legally accessible time-sensitive information. The more open the society and the more transparent the respective regime, the more open and robust information it will produce. Still, penetrating closed societies in many cases is much more relevant for intelligence.

2. Open sources per definition emit much more visible information than non-open sources, albeit only in quantity and not necessarily in quality.

3. With the advent of new media (going hand in hand with a massive decline in plain text information), the variety, volume and velocity of information multiply. Organizing this overflow continues to be the single most pressing challenge of OSINT, even more so in the wake of the information revolution.

4. Media are, in the absolute majority of cases, means to transport information, not sources themselves (the internet is generally not a source as opposed to a specific website).

5. Due to the nature of threats especially during wartime, most of the information relevant for national security and defense is found in foreign sources, and not readily at hand in domestic ones. To exploit those sources, collectors and analysts need adequate training, appropriate literacies and skills (what to look for, how to get and understand it) to put the disparate pieces of raw data into context and make sense of them. In no other intelligence-related area it is less delicate to employ independent contractors with specialized expertise to meet the requirements.

6. Information that is exclusively collected or acquired through open sources and means can be shared with both the public (for example to justify political decisions or to measure their public impact) and other – even foreign – organizations and agencies (for example to verify and validate information or targeting further secret collection) at discretion. It might still be classified for strategic reasons, such as disguising one's search intent.

7. Collecting information from open sources is generally less expensive and less risky than collection from other intelligence sources.

8. Identifying what is not publicly available or legally accessible also is a value-added through OSINT, making it a choice of *first resort*. OSINT is more than press clippings.

9. As information is the medium of exchange in international intelligence relations, fusing open information can help to override isolated silo-thinking and cultural

NOTES

bias, thus broadening the scope of collection and deepening the explanatory power of analysis for the sake of national security.

Consequences for National Security as a Public Good

National security must be seen as a *public good*, to be provided efficiently only under state supervision or by the government itself. Thus, intelligence - serving national security - requires at least a government mandate and control. As soon as this requirement is not given, the term has to be put explicitly in an alternative context (e.g. private, business or competitive intelligence) serving solely non-state interests. Here, intelligence is only discussed insofar as it serves national security.

Since modern economic theory postulates that efficient state action presumes market failure, it would be necessary to analyze whether and where the state is actually able to provide better intelligence than non-state players. However, in case the state is inferior to the market in terms of its capabilities or resources, a non-state provision can be efficient. Yet, this would require state regulation.

Assuming that a government may have extended legal authority, but not necessarily more resources or capabilities than non-state players, implies that those special permissions are the actual distinctive criterion between the government and the public in terms of intelligence oversight and provision. Thus, unless the government endows non-state contractors with special permissions to fulfill a specific task, OSINT, as intelligence which is generated exclusively using sources openly available *and* legally accessible by the public, remains the only sort of intelligence which can be provided by non-state players. Intelligence derived using sources and means which are openly available but not legally accessible to the public must not be considered OSINT, e.g. leaks, the legal status of which are in question.

It must be concluded that the *general public* cannot contribute anything of value to the intelligence requirement as long as it has fewer permissions and no superior expertise. This, of course, calls for the government to be at least as qualified as the general public, a prerequisite which nevertheless does not hold true in some cases. One example for inferiority of the government to the general public is an insufficient tech-savviness and internet access of some departments. Fortunately, the prevailing capability and qualification deficiency of government bodies becomes only obvious in comparison with a sufficiently skilled or endowed part of the public. Therefore, it is mainly this *specialized public* (including cases of *serendipity*) which can constitute missing sources and means for the intelligence community.

In consequence, while representing a special challenge for both sides, *Public-Private-Partnerships (PPPs)* may be aspired in an intelligence market as an efficient alternative to intelligence exclusively provided by the state itself. Nevertheless, the crucial point in such partnerships is an increased emphasis on clearance, classification and any form of non-disclosure protection which still must be executed by the government, due to the extreme portability and strategic potential of information. Again, sometimes, even an intelligence product based solely on openly available information must be classified to protect the government's interest from being revealed. Thus, the key challenge is to find an optimal equilibrium between sealing and opening a national intelligence enterprise. While national security must remain the primary goal of intelligence communities, it is a combination of two main strategies - *hide and seek* - which does lead to the aspired informational dominance but at the same time bears an inherent risk for both strategies to endanger one another, thus potentially compromising the supreme mission to effectively serve national security. Having this in mind, intelligence directorates must integrate outsiders' capabilities through effective directives which regulate outreach activities and all sources exploitation without jeopardizing operational and national security.

Partnerships with academia can mitigate potential conflicts of interest between the state and non-state players. While the state aspires to common welfare, individuals from the public primarily follow their own interests. However, the academic world does rather not aim at profit maximization but at the extension, accumulation and distribution of knowledge. This makes universities the most fertile ground for diverse expertise within the public sphere and ideal partners for the IC. The so called *Centers of Academic Excellence (CAE)*, which are part of a university program to recruit the best experts from diverse backgrounds for the US IC, represent a good example for such an approach.

NOTES

Seeing intelligence provision as tradecraft – comprising both analysis and collection of relevant information – calls for an effective training by experts and an exchange of best practices between intelligence professionals. The imperative to exploit all sources for relevant information to feed given intelligence requirements and the fact that open sources often provide the majority of intelligence input, though not necessarily the *dot on the i*, makes OSINT an essential part rather than a specialty of tradecraft, which must be commanded by every intelligence professional, even more so as analysis and collection are increasingly merging with each other. Nevertheless, outreach activities and open source exploitation have to be supported by respective specialized elements within the IC to ensure that analysts are keeping up with the market. Elements specialized in OSINT are most qualified to identify potential capability gaps in comparison with the public and to assess where contractors can be of use. A good way to better integrate the necessary knowledge and skills into the IC would be an OSINT certification program, currently being introduced in the US for example. If PPPs do not qualify for intelligence provision because the risk of compromising operational or national security appears too high, they may still work for providing training and information about new publicly available sources, means and research of potential relevance without uncovering critical information about the IC's structure, resources, intentions and activities. In any case, coordinated outreach and open sources exploitation endeavors do lead to more awareness for inefficiencies. The required comparison of state and non-state capabilities, of course, initiates a competition which generates an improved allocation of national security at the price of a certain discomfort due to a questioning of the status quo and the resulting changes.

New Challenges

Since intelligence services must not only keep up with non-state capabilities but also with adversaries and foreign services, getting in touch with opponents, competitors, partners and the public is unavoidable and should be addressed proactively to prevent both being spied on and falling behind. In the aftermath of 9/11, intelligence failures - particularly a deficient consideration of OSINT - have been identified as major reasons for the inability to anticipate and prevent these attacks which were immediately followed by ongoing large-scale and high-intensity interventions from the US and NATO. Ever since, 9/11 has been taken as the turning point for most nations' defense strategies and has initiated massive reforms of the US IC following the *Intelligence Reform and Terrorist Prevention Act (IRTPA)* from 2004, which also mandates the creation of the OSC in 2005. New asymmetric threats require more broadly focused information awareness, increased international cooperation of ICs and the integration of all relevant expertise - challenges to which OSINT, essential to the all sources intelligence tradecraft, can indeed contribute substantially. Concepts such as *comprehensive security* (German: *Vernetzte Sicherheit*) are being discussed and successively implemented within national security communities of different countries and increasingly determine international collaboration. Nevertheless, the interrelation between OSINT and comprehensive security is often not yet identified sufficiently.

Most noteworthily, in the US, the Office of the DNI has issued a number of respective *Intelligence Community Directives (ICDs)* in the last four years, which have established a *National Open Source Enterprise* under the ADDNI/OS who is also responsible for encouraging community collaboration and building PPPs, implemented *Human Intelligence* (HUMINT) standards including overt sources and means, commanded active outreach, engagement, networking and convenient internet access to engage outside expertise, as well as the flexible appointment of so called *Highly Qualified Experts* (HQEs). Thereby, on the one hand, the DNI explicitly prohibits the assignment of outside HQEs to provide expertise which is readily available within the IC. On the other hand, he assumes that there is expertise needed to satisfy emerging and non-permanent requirements which can only be provided by external HQEs. While those contracts are tailored on a case-by-case basis, they constitute employment with the ODNI with the goal to reduce reliance on contract personnel for missing expertise. Thus, those experts would fall under federal authority, oversight and tighter control.

Each nation's IC has its own approach to the interdependencies of outreach, secrecy, quality management and relevant sources exploitation, while not all governments do issue respective directives as unclassified. However, it seems that most nations do not address those challenges in such an

NOTES

explicit and comprehensive way as the US. The aforementioned challenges contribute much to the ambivalent role of OSINT in ICs. Even in the US, OSINT-related resources are still insufficient, although even higher echelons have emphasized the importance of OSINT repeatedly. Yet, intelligence consumers seem to appreciate intelligence all the more when it is enriched by information exploited from clandestine sources and means, while the very producers of this intelligence seem to have a better awareness of the actual value-added of OSINT. Besides the need for an increased horizontal exchange with outsiders and other state elements, a vertical exchange throughout the entire hierarchy within the IC and other relevant departments must be fostered as well. This assures the required awareness to consider all relevant human or technological sources and means in intelligence products efficiently serving national security.

Such an IC-wide awareness for open sources and means is even more important when facing adversarial states with less open societies, as they provide far less relevant and reliable information but can, in turn, profit from a relatively high detail of information serving their hostile interests. Obviously, this is a double strategic disadvantage for open societies, as they will not only be more prone to attacks but also do not have access to the same detail of relevant information. In addition, in democracies the public is a government's ultimate protégé and sovereign and thus its major critic. In case of intelligence failures the public comprehensibly shows no understanding as long as the government's decisions are not transparent and the public had no possibility to intervene in advance. A democratically elected government will lose its credibility and authority without the support of its people, while non-democratic governments do not have to fear this pressure. Openly available and legally accessible information thus helps governments preserving their credibility and justifying their decisions to the public and international allies. An increased awareness of a more and more dynamic and complex public information distribution and its consequences is an absolute must for ICs. Although, fast developing information technology plays an important role in this challenge, the human factor must not be underestimated. In most cases, technology cannot yet replace human assessment of information, and decisions of relevance for national security should certainly not be based on automatically selected and evaluated information without properly understanding the underlying processes. Ultimately, it will always be human expertise that really makes the difference in the intelligence tradecraft. Open societies have one unbeatable strategic advantage in comparison to unfree and often hostile nations: their human capital. For this reason, intelligence communities are called to incorporate all relevant expertise from its actual origin: the public.

NOTES

Sources and Links

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: Intelligence Analysis in the Knowledge Age. (2010)
http://scholar.sun.ac.za/bitstream/handle/10019.1/3087/Duvenage,%20M.A.pdf?sequence=1

Stevyn Gibson: Open Source Intelligence - An Intelligence Lifeline. (2004)
http://www.rusi.org/downloads/assets/JA00365.pdf

Arthur S. Hulnick: The Dilemma of Open Source Intelligence - Is OSINT really intelligence? in: Loch K. Johnson (ed.): The Oxford Handbook of National Security Intelligence. (2010)

William J. Lahneman: The Need for a New Intelligence Paradigm. in: International Journal of Intelligence and Counter-Intelligence. Volume 23, Issue 2. (2010)

LexisNexis Open Source Intelligence Roundtable: OSINT 2020 - The Future of Open Source Intelligence. (2010)
http://www.dni.gov/speeches/Speech_OSINT_Roundtable_20100617.pdf

Stephen C. Mercado: Sailing the Sea of OSINT in the Information Age. (2004)
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html

Harris Minas: Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century? (2010)
http://rieas.gr/images/rieas139.pdf

NATO Open Source Intelligence Handbook. (2001)
http://blogs.ethz.ch/osint/files/2010/08/nato-osint-handbook-v12-jan-2002.pdf

Anthony C. Olcott: The Challenges of Clashing IC Interests. in: International Journal of Intelligence and CounterIntelligence. Volume 23, Issue 4. (2010)

Joseph E. Roop: Foreign Broadcast Information Service History. (1969)
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/foreign-broadcast-information-service/index.html

Brian Rotheray: A History of BBC Monitoring. (2009)
http://www.monitor.bbc.co.uk/about_us/BBCMhistory%20revisions%20x.pdf

Noah Shachtman: Open Source Intel Rocks — Sorry, It's Classified. (2008)
http://www.wired.com/dangerroom/2008/09/download-hayden/

Jan Störger: Die Rolle von Open Source Intelligence im Rahmen deutscher Sicherheitsinteressen. (2008)
http://osintwiki.org/index.php?title=Die_Rolle_von_Open_Source_Intelligence_im_Rahmen_deutscher_Sicherheitsinteressen

United States Department of the Army: Open Source Intelligence FMI 2-22.9. (2008)
http://ftp.fas.org/irp/doddir/army/fmi2-22-9.pdf

United States Department of Defense Instruction No. 3115.12: Open Source Intelligence. (2010)
http://www.dtic.mil/whs/directives/corres/pdf/311512p.pdf

United States Intelligence Community Directives No. 301 (2006), No. 205 (2008), No. 304 (2008), No. 623 (2008), No. 612 (2009)
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

Kurt Werren, Kian Fartab: All Sources Collection – Kernstück eines leistungsfähigen Nachrichtendienstes. (2010)
http://www.asmz.ch/fileadmin/asmz/ASMZ_aktuell/2010_04/All_Sources_Collection_Deutsch_1_.pdf

Robert L. Worden: United States Federal Research Division - Gathering Multidisciplinary Information for the Policy-Making Community. (2006)
http://www.loc.gov/rr/frd/pdf-files/info_for_policymakers.pdf

NOTES

ISN
ETH Zurich

INTERNATIONAL RELATIONS AND SECURITY NETWORK

ETH Zurich | Leonhardshalde 21, LEH | 8092 Zurich | Switzerland
Tel: +41 (0)44 632 04 24 | Fax: +41 (0)44 632 14 13
www.isn.ethz.ch | osint@sipo.gess.ethz.ch

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich