REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-04-2018	Master's of Military Studies	SEP 2017 - APR 2018

4. TITLE AND SUBTITLE

Overcoming Information Overload: Open Source Intelligence in a Modern Threat Environment

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Minner, Scott D., DIA

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
John Gordon

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The changing nature of global threats to the United States and an evolving information environment require fundamental adjustments to intelligence structures and processes, and open source intelligence (OSINT) offers the most adaptive and expansive discipline to address these global changes. Four underlying issues establish the basis for elevating OSINT as an intelligence discipline: 1) the blurred line between intelligence and information; 2) the need to adjust the intelligence community (IC) to a changing environment; 3) the vast array of threats in a globalized environment; and 4) the exponential growth of the information environment. OSINT offers the most effective approach to address these issues, though it cannot address all or even the most dangerous threats. A dual track approach of OSINT and focused secret intelligence disciplines through a combination of pragmatic, targeted solutions and incremental restructuring offers the most likely chance of negotiating today's threat environment.

15. SUBJECT TERMS

OSINT; Information Revolution; Open Source; threat environment; information environment; intelligence community

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			USMC Command and Staff College
UNCLASS	UNCLASS	UNCLASS	UU	38	**19b. TELEPHONE NUMBER** *(include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: Overcoming Information Overload: Open Source Intelligence in a Modern Threat Environment

SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Scott Minner

AY 2017-18

Mentor and Oral Defense Committee Member: Dr. John Gordon
Approved: _____
Date: 4/18/18

Oral Defense Committee Member: Mr. Michael Cicere
Approved: _____
Date: 4/18/2018

dsbjorn Leysgard. USDOC.

Paul M. Christon 4/18/2018

Executive Summary

Title: Overcoming Information Overload: Open Source Intelligence in a

Modern Threat Environment

Author: Scott Minner, Defense Intelligence Agency

Thesis: The changing nature of global threats to the United States and an evolving information environment require fundamental adjustments to intelligence structures and processes, and open source intelligence (OSINT) offers the most adaptive and expansive discipline to utilize the information age to address the scope of U.S. national security interests.

Discussion: Four underlying issues establish the basis for elevating OSINT as an intelligence discipline. First is the increasingly blurred line between intelligence and information as the latter becomes increasingly overwhelming. Second is a need to adjust perspective on the purpose of the U.S. intelligence community (IC) to adapt to a constantly changing global environment. The third and fourth issues address the nature of that environment. The post-Cold War security environment includes a vast array of both symmetric and asymmetric threats to U.S. national interests, which themselves are increasingly complex and interrelated in a globalized world. Simultaneously, the information environment from which the IC must draw conclusions about those threats is growing exponentially. Given these factors, OSINT is the only intelligence discipline that offers a realistic approach to maintaining U.S. interests.

The need for traditional IC structures and processes is not diminished, however. OSINT offers the most effective approach to address expansive threats and information, but it cannot address all or even the most dangerous threats. Recognizing the need for a dual track approach to intelligence and the difficulties of extensive reform, a combination of pragmatic, targeted solutions and incremental restructuring offers the most likely chance of successfully establishing OSINT dominance in the U.S. intelligence apparatus of the Information Age.

Conclusion: The U.S. IC and policymakers understand the importance of open source information, but the IC has not adapted its culture and practices to address it. A continued focus on traditional, secret intelligence disciplines hampers the IC's ability to keep pace with the vast amounts of information or address the preponderance of threats the U.S. faces today. Rigorous OSINT development and changes to processes and training necessary to provide it will be critical if the IC is to continue its primary function of preventing strategic surprise to U.S. interests.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Tables

Page

Illustrations

Page

Table of Contents

Page

Preface

When considering the concept of "military revolutions" during my time at Marine Command and Staff College, I began to think about revolutions in intelligence affairs. I tried to determine what the next revolution in intelligence would be and what the IC would look like years from now. What I realized, however, is that the IC still fundamentally functions as it did during the Cold War despite constantly changing security and information environments.

The IC has certainly adapted in the face of particular threats, most notably in 2004 with the establishment of the Director of National Intelligence. Most of these changes, however, have been reactionary and have not reassessed the purpose of intelligence nor have they addressed the fundamental processes of the IC in the face of a changing global environment.

My approach to understanding this problem solidified during an elective course on strategic surprise, in which we studied theories of intelligence and the underlying tenets of intelligence failure in the context of well-known case studies. I realized the entire purpose of the IC, and therefore its approaches and processes, is outdated and must be reassessed.

Acknowledgments

I would like to thank Mr. Mike Cicere for reminding me why intelligence professionals do what we do, and Dr. John Phillips and Dr. Anne-Louise Antonoff for helping me to understand the nature of conflict and its place in a changing world. I would also like to thank Mr. Andy Roberts and Mr. Bill Kerner at DIA and Dr. Melissa Burn at MCIA for sharing their extensive expertise on OSINT and making me feel a little better about where the IC is going. Thank you to Dr. Gordon for his help getting me through this research. Finally, I would like to thank my wife, without whom my ideas would not read nearly as well.

Knowledge is change—and accelerating knowledge-acquisition, fueling the great engine of technology, means accelerating change.[1]

Alvin Toffler, 1970

On balance, the post– Cold War world promises to be a messy one where violence is common, where conflicts within and between nation-states abound, and where the question of U.S. military intervention becomes more rather than less commonplace and more rather than less complicated.[2]

Richard Haass, 1998

OSINT is the edge pieces of a jigsaw puzzle, which is necessary to start and finish the puzzle.[3]

Dr. Joseph Nye, Jr., Chairman of the National Intelligence Council, 1993-1994

The United States National Security apparatus is tasked to protect U.S. national interests, not the least of which are the lives and liberties of American citizens. The U.S. government chiefly looks to its military instrument of power to protect its citizens from threats and to its Intelligence Community (IC) to monitor those threats or, to paraphrase Roberta Wohlstetter's seminal study of Pearl Harbor, to differentiate the "signal" from the "noise."[4] The information and threat environments in which the IC must do so, however, have evolved more rapidly than the IC has been able to adapt. The Information Revolution (defined here as "the explosion of the availability of information due to the use of computers, the Internet, and other electronic devices"[5]) and the fall of the Soviet Union in particular have so drastically altered the landscape that the IC's traditional focus on secrets and spies struggles to address all of the threats and to identify all of the signals. Open source intelligence (OSINT) offers an intelligence discipline that can capture all of the "noise" necessary to address all the threats, but a conscious effort to

improve the utilization of OSINT on the part of both the IC and the national security apparatus it informs is needed to identify the signals.

The IC's structure and basic functions remain holdovers from the days of the Cold War, with the IC intelligence cycle focused on collection feeding analysis. As applied to covert and technical collection on state-based adversaries, the traditional cycle works. The Information Revolution, however, has not led to an increase in secrets, but an increase in the amount of publicly available information (PAI). Beneficiaries of revolutions in military or intelligence affairs are those states that can adapt to changing circumstances and technologies to gain an advantage over their adversaries. In the case of intelligence, that advantage is an ability to anticipate threats to U.S. strategic interests to enable both preemptive and responsive policy. In the information environment of the 21st century, changes to how the IC handles OSINT must be at the forefront of reappraisals of IC structures and processes.

This study will first define OSINT and establish its place in the pantheon of intelligence disciplines by demonstrating its inherent strengths. It will then identify critical shifts in both the global threat and information environments and demonstrate the IC must fundamentally adjust its approach to intelligence collection and analysis to achieve its primary purpose of preventing strategic surprise. Finally, it will address the current challenges to bolstering OSINT within the IC and offer several potential solutions (both systemic and targeted) to address shortfalls. Ultimately, this study will demonstrate that the IC, though cognizant of OSINT strengths and relative importance, must further prioritize OSINT development at all levels to protect U.S. national interests.

What is OSINT?

To determine how best to utilize OSINT, a common definition is required. The Office of Director of National Intelligence (ODNI) website identifies OSINT as one of six intelligence disciplines (i.e. collection methods): human (HUMINT); signals (SIGINT); imagery (IMINT); geospatial (GEOINT); measures and signals (MASINT); and open source (OSINT). ODNI defines OSINT as "publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings."[6] Modern practitioners, however, differentiate OSINT as the intelligence analysis of publicly available information (PAI).[7] Disparities in definitions therefore raise the question: What is the difference between intelligence and information?

Where does OSINT fit?

For at least the last decade the IC and policymakers have recognized the importance of OSINT. The Intelligence Reform and Terrorism Prevention Act of 2004 noted that, "Open-source intelligence is a valuable source that must be integrated into the intelligence cycle to ensure that United States policymakers are fully and completely informed."[8] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction further stated, "The need for exploiting open-source material is greater now than ever before… The ever-shifting nature of our intelligence needs compels the Intelligence Community to quickly and easily understand a wide range of foreign countries and cultures… The Intelligence Community must make a concerted effort to solve the technology and security challenges associated with getting open-source information to every analyst's desktop…"[9] Today, OSINT is an integral part of intelligence analysis, potentially accounting for 80-95 percent of U.S. finished all-source intelligence analysis.[10]

OSINT Strengths

OSINT has several inherent strengths that distinguish it from the other intelligence disciplines. While these strengths have evolved over time, they are still fundamentally similar to the strengths OSINT offered in World War II:

- **OSINT is often the only available source** due to limited priorities and resources for intelligence collection. In a world where threats can come from almost anywhere, the IC simply does not have enough technical or human collection assets to cover everything.
- **OSINT is quickly accessible**. Unlike secret collection methods, open source information is being collected and disseminated on almost any topic every day by other organizations and individuals around the world. With the proper tools and training, much of that information is available almost instantaneously.
- **OSINT can tip or cue additional secret collection assets**. Due to the availability and accessibility of open source information, analysts can use OSINT to identify important issues to which the traditional intelligence cycle of collection and analysis can be more efficiently applied.
- **OSINT is easily shareable**. The customer base of the intelligence community, including defense intelligence, has expanded as threats and the means to counteract them have expanded. Generally, the IC and the defense community does not operate domestically and cannot share its sources and methods with law enforcement. The same applies to foreign partners, with whom the U.S. has limitations on what secret information can be shared. By utilizing OSINT, however, intelligence information

and analysis can be easily disseminated to those decisionmakers and actors who can use it.

Why OSINT?

Four overarching issues determine the shape that OSINT should take. The first, already identified, is the difference between intelligence and information. If the two are the same, what is the purpose of the IC? Secondly, and deriving from the first, is the inherent purpose of intelligence. It is impossible to determine how to best utilize OSINT without fully understanding why the intelligence community exists in the first place. Third, what is the nature of the threat? An IC focused almost exclusively on the Soviet Union, for example, looks vastly different from one monitoring the multiple, global threats described in the 2018 National Defense Strategy.[11] Finally, what is the nature of the information environment? How is information disseminated and consumed? This final piece helps to shape OSINT as it relates to the other intelligence disciplines and its overall place in IC policy.

Intelligence vs. Information

The ODNI website identifies a broad, conflated view of intelligence and information. Intelligence is "information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security."[12] Under this view, in the cases of HUMINT, SIGINT, MASINT, IMINT, and GEOINT, part of the distinction between intelligence and information is in the method of collection. Intelligence is information collected in a secret or sensitive manner, which must be protected. In the case of

OSINT, however, when the source of the intelligence is publicly available to all, should it still be considered intelligence?

As noted above in regard to OSINT specifically, modern practitioners define intelligence as the analysis of information. A 1996 OSINT training manual from DIA's Joint Military Intelligence Training Center (JMITC) provides more specifics. Information, according to the manual, is "[d]ata (raw print, image or signal) that has been collated, processed, in order to produce a report that is of generic interest." Intelligence is "[p]roducts which tailor information in order to support a specific decision by a specific customer."[13] The updated version of the same manual defines open source information as "PAI that anyone can lawfully obtain by request, purchase, or observation." OSINT is "PAI that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[14] As seen in these definitions, intelligence, even OSINT, is not just information but the processing and dissemination of that information to inform policy, regardless of the method by which it is collected. The IC, then, has an obligation to incorporate OSINT into the analysis provided to customers.

Intelligence Has a Purpose

The purpose of intelligence is not a simple matter. Numerous volumes have been written trying to delineate theories of intelligence and to differentiate intelligence and information. Even more ink (and blood) has been spilled in both official and unofficial channels trying to get intelligence right, be it through new structures, processes, technologies, or all of the above. The post-World War II debates and bureaucratic politics that eventually led to the establishment of the Central Intelligence Agency (CIA) in 1947 provide an understanding of what constitutes the

U.S. government's purposes for intelligence. Many government officials were reticent to establish a permanent, peacetime intelligence organization, following in the same footsteps as former Secretary of State Henry Stimson, who famously stated in 1929 that, "Gentlemen do not read each others' mail."[15] President Truman, meanwhile, may have been influenced to disband the wartime Office of Strategic Services (OSS) due to concerns over the potential for an "American Gestapo."[16]

Truman eventually realized the importance of a permanent intelligence function, particularly in the face of an anticipated Soviet threat, and established the Central Intelligence Group in 1946 and its successor, the CIA, in 1947. As he later noted in his memoirs, Truman "often thought that if there had been something like coordination of information in the government it would have been more difficult, if not impossible, for the Japanese to succeed in the sneak attack at Pearl Harbor."[17]

Mark Lowenthal, in his book *Intelligence: From Secrets to Policy*, synthesizes the essence of those post-World War II debates into four key functions of intelligence:[18]

1. To prevent strategic surprise.
2. To provide long-term expertise.
3. To support the policy process.
4. To maintain the secrecy of information, needs, and methods.

Three of Lowenthal's four functions apply to the full spectrum of intelligence disciplines (as noted in the previous section, the fourth function inherently does not apply to OSINT). His second and third functions identify the IC's obligations to maintain knowledge, both historical and current, from all sources to inform decisions. Lowenthal's first function, however, provides the basis upon which a strong foundation in OSINT must be built, and it is informed by the

nature of modern threats.

The Nature of the Threat

To understand the nature of the threat, we must consider the concept of strategic surprise and its prevention (Lowenthal's first function). As evidenced by President Harry Truman's memoirs, he built the foundations of today's IC due in no small part to the desire to prevent another Pearl Harbor. The most recent major reforms in the IC in 2004, particularly the establishment of the ODNI, stemmed from the surprise terrorist attacks on September 11, 2001. Threats have obviously evolved since 1947, but the pace of change since 2004 has been no less dramatic. The question, then, is what is strategic surprise in the 21st century, and what are the threats leading to it?

"New war" theorists argue that conflict in a post-Cold War, globalized environment, is "substantively distinct" from older forms of conflict.[19] A study conducted by the Strategic Studies Institute of the U.S. Army War College identified many of the new factors, noting "the number of actors simultaneously empowered to resist U.S. influence effectively, the variety of routes and vectors from which they can threaten harm to core U.S. interests, and, finally, the volatility of an international system under persistent seismic pressure from the competing forces of integration and disintegration."[20] As Erik Dahl noted in an interview regarding his book *Intelligence and Surprise Attack*, the world has significantly changed since the strategic surprise of the attack on Pearl Harbor in 1941. The ultimate aim of the national security apparatus now may no longer be a focus on avoiding future Pearl Harbor-like attacks from state actors, but an aim to maintain the security of American citizens and interests globally.[21] Furthermore, the 2018 National Defense Strategy acknowledges "an increasingly complex global security environment,

characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations. These changes require a clear-eyed appraisal of the threats we face, acknowledgement of the changing character of warfare, and a transformation of how the Department conducts business."[22] A definition of strategic surprise should therefore encompass a broad multitude of threats and should inform the future direction of U.S. intelligence, particularly the role of OSINT.

Historical and disparate definitions of strategic surprise are obsolete but still inform current IC structures and processes. They focus largely on foreign state-based threats and their influence is demonstrated in the current Joints Chiefs of Staff "4+1" threat framework: Russia, China, North Korea, Iran, and violent extremism.[23] Mark Lowenthal's own definition of strategic surprise is "threats, forces, events, and developments that are capable of endangering the nation's existence," and he therefore discounts September 11, 2001, considering it "not of sufficient magnitude and importance to threaten national existence".[24]

Another student of strategic surprise, Ariel Levite, draws from other scholars to provide a broad definition of strategic surprise: "a sudden realization that one has been operating on the basis of an erroneous threat perception… [which] occurs through failure to predict, much less anticipate, an acute and immediate foreign threat to the 'vital' national interests."[25] He then delineates essentially six key elements of strategic surprise:[26]

1. A discrete case.
2. A failure to anticipate immediate threats from hostile and peaceful actions.
3. The deliberate intent of surprise by a perpetrator.
4. Participants are aware of values at stake.
5. Along one or more of five dimensions (Who? What/how? When? Where? Why?).

6. Due to failures at either intelligence or policy levels.

Each of these definitions highlights the grave threat of strategic surprise, but either no longer applies or misapplies the concept to today's threat environment. By applying Lowenthal's definition to his four functions, any threat that falls below the threshold of threatening national existence should not be a focus of the intelligence community. Furthermore, he fails to adequately address long-term consequences as opposed to immediate effects in his example of September 11, which shattered the American illusion of safety and led to two wars that continue to shape U.S. policies and the international system. Levite's definition more accurately identifies threats to "vital interests", but limits the scope to foreign threats. Levite offers a useful rubric upon which to grade strategic surprises, but his framework misses critical examples, such as the fall of the Soviet Union, that do not adhere to "deliberate intent" or "immediate threats."

Strategic surprise is a failure to anticipate or prepare for a discrete event that causes significant loss of American lives or severe consequences to American national interests. As an alternative framework for analyzing strategic surprise, this definition addresses some of the problems outlined above. Threats do not have to be foreign or state-based, nor does a strategic surprise event have to be deliberate or nefarious. This definition, though broad, helps to characterize the nature of today's threats in a complex, interconnected, globalized world.

The Information Environment

The fourth and final factor influencing intelligence disciplines, and OSINT in particular, is the shape of the information environment. Commonly referred to as the Information Revolution, today's information environment continues to expand at an astronomical rate. In 2010, Eric Schmidt (CEO of Google) stated that every two days, people create 5 exabytes of

data, or roughly the same amount of information created from the dawn to civilization until 2003.[27] A common refrain from big data analytics companies like IBM is that at any given time 90 percent of the world's information was created in the previous two years.[28]

The nature of the information environment has also changed. Whereas previously OSINT analysts could focus primarily on official news sources, the advent of the internet and, more currently, social media and mobile devices has diminished costs of transmission and leveled the playing field for information dissemination. Therefore, not only are there more communications but also ever-expanding purposes and audiences for information. In 1948, Harold Lasswell and other members of the Rockefeller Foundation's Communication Group developed a formula (known as the "Lasswell formula") that assigns five parts to any act of communication: 1) Who? 2) Said what? 3) In which channel? 4) To whom? 5) With what effect?[29] For the purposes of OSINT, Lasswell's formula serves as a form of source validation, causing analysts to question the validity and intent of the information being disseminated. Since 1948, however, the focus of the formula has shifted.

In his book *Open Source Intelligence in a Networked World,* Anthony Olcott argues that OSINT within the IC initially focused on the "transmission model" of communications theory, utilizing propaganda analysis to understand radio broadcasts from Berlin and Tokyo. Two key elements establish the foundation of propaganda analysis: 1) propaganda is strictly controlled and 2) constant monitoring enables analysis of changes. By monitoring all of an adversary's official broadcasts and comparing them to real world events, OSINT analysts were able to provide insights into shifts in the enemies' tones and attitudes.[30] [31] The basic foundation of the transmission model was that, at the time of the foundation of IC OSINT, the costs to transmit to large audiences was far more expensive than to receive and therefore analysis was able to focus

on the relatively few channels of communication.[32]

Today, the costs of transmission and reception have achieved parity. Nearly anyone can communicate whatever they want to as large an audience as is willing to pay attention. In this new information environment, Olcott argues the "uses and gratifications" theory of communication is more applicable, suggesting the audience is the more important focus than the source, as consumers dictate whether messages resonate.[33] The Lasswell formula still applies here, but the potential answers to the questions, particularly "to whom?" and "to what effect?" are more difficult to ascertain. OSINT, therefore, must address not just the volume but also the nature of the information environment to validate analytical conclusions.

History of OSINT

The history of OSINT provides an understanding of the issues that plague the OSINT discipline and the many efforts that continue to try and address them. The formal history of OSINT within the U.S. government begins with the Foreign Broadcast Monitoring Service (FBMS). In 1941, Assistant Secretary of State Breckinridge Long tasked the Federal Communications Commission to begin monitoring foreign radio broadcasts as well as domestic ones. Domestic operations had been largely focused on monitoring subversive messaging emanating from within the U.S., but U.S. officials realized that foreign broadcasts, including Nazi and fascist propaganda, was reaching U.S. listeners.[34] Initially, FBMS established listening outposts around the country focused on particular areas of the world (e.g. the West Coast focused on Japan) and provided daily digests of translations and summaries. FBMS also experimented with its own analysis of foreign broadcasts, which it published on a weekly basis, to include a December 6, 1941 review that warned Japanese radio had "dropped its tone of caution and was

assuming a belligerent attitude."[35]

FBMS changed its name to the Foreign Broadcast Intelligence Service (FBIS) in 1942 but remained under the FCC. During these early days, FBMS/FBIS experienced several of the issues that continue to plague OSINT to this day. Chief among them was the lack of language capability. At the time, the primary difficulty lay in the lack of trust the U.S. government placed in those with the necessary language skills, particularly Japanese Americans. FBIS was also plagued by bureaucratic politics, constantly fighting turf battles with the Office of War Information (OWI; tasked with U.S. propaganda and information efforts), and embroiled in bureaucratic politics regarding where the agency should be placed.[36]

The primary point of contention between OWI and FBIS was who should be conducting the analysis of foreign broadcasts. FBIS analysts felt they were best placed to both monitor and analyze, while OWI's Bureau of Research and Analysis (effectively a customer of FBIS reports) felt it should "[control] the full process of the analysis." A compromise between the two in October 1942 led to collocation of the Analysis Division of FBIS with OWI but gaining sole responsibility for analysis.[37]

Given the origin of the agency's mission, FBIS focused heavily on official radio broadcasts from other countries, much of which was propaganda. Many decisionmakers at the time (and to this day) questioned the utility of an agency that only had access to material readily available to the public. This led FBIS to develop a unique approach to analysis that exemplifies the utility of OSINT expertise: propaganda analysis.

Simultaneously, the Office of Strategic Services (OSS) developed an open source analysis branch called Research and Analysis (R&A). Over the course of R&A's four year existence, the branch produced over 2,000 reports, ranging from the attitude of the Roman

Catholic Church in Hungary to inflation in Burma.[38] R&A's most notable contribution (and one that reportedly continued through OSS's evolution into the Central Intelligence Agency) was an ability to cross-index tens of thousands of documents in order to produce detailed open-source analysis on order in a relatively short period of time.[39] Unlike FBIS, however, R&A did not solely focus on radio broadcasts and relied heavily on a separate collection branch of OSS, the Interdepartmental Committee for the Acquisition of Foreign Publications (IDC), which acquired vast amounts of raw data and documents for R&A analysis. FBIS did have a counterpart division within FCC, the Foreign Documents Division, whose purpose was similar to that of the IDC, but FBIS and FDD only occasionally collaborated.[40]

Post-World War II, both FBIS and R&A were caught up in the philosophical debates and bureaucratic politics surrounding the idea of peacetime intelligence. R&A was eventually disbanded, though some elements shifted to the Department of State's Office of Research and Intelligence while some individuals later helped to establish the CIA's Directorate of Intelligence.[41] FBIS (and FDD) shifted from the FCC to the War Department in January 1946, though this arrangement was only temporary until June 1946, when they shifted once again under President Truman's new Central Intelligence Group.[42] Finally, in 1947, FBIS and individuals previously associated with R&A came under the new Central Intelligence Agency, which took over all elements of the CIG under the National Security Act of 1947.[43]

FBIS continued operations as the primary open source element of the IC, slowly adapting along with advances in information and communications, until 2005 when DNI John Negroponte created the Office of DNI's Open Source Center (OSC). The OSC largely retained the evolved functions of FBIS, with the previous director of FBIS becoming the first director of the OSC, but the rebranding served to highlight the expanded nature of OSINT in the 21st century. OSC's

stated mission included "collection, analysis and research, training, and information technology management to facilitate government-wide access and use."[44] The DNI further rebranded OSC into the Open Source Enterprise (OSE) in 2015, though OSE remains under the Director, CIA as the lead open source functional manager.[45] [46]

Highlighting an increased focus on integration and interagency cooperation, in 2006 the DNI established the National Open Source Enterprise (NOSE) and National Open Source Committee (NOSC) with Intelligence Community Directive (ICD) 301 under an Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS).[47] Following suit, in 2010 the Department of Defense created the Defense Open Source Council (DOSC) to coordinate defense intelligence OSINT policies with the Director, Defense Intelligence Agency as the DoD lead component for OSINT.[48] ICD 301 was rescinded in 2012, but the NOSC continues to function as the primary OSINT coordination body of the IC.[49]

Ongoing Challenges

The history of OSINT and the nature of today's information environment highlight numerous challenges for the OSINT discipline:

Quantity and Complexity: The sheer volume of PAI and the various forms it takes overwhelm the traditional intelligence cycle and methods of collecting and processing information into analysis.

Source Attribution: With the vast amounts of information available, analysts can have difficulty differentiating good from bad sources. As identified in numerous studies of strategic surprise and intelligence failures, separating the signal from the noise becomes increasingly difficult the more

information is available. Even when analysts are able to identify a good open source, the ability to convey the quality of the source becomes increasingly difficult as the sources become increasingly esoteric. Studies of strategic surprise, such as Wohlstetter's study of Pearl Harbor, emphasize the importance of decisionmakers' appreciation of source quality.

Languages: Problems with language translation are not unique to OSINT. SIGINT inherently requires language capabilities from translators. HUMINT often requires some amount of language ability from collectors. SIGINT and HUMINT, however, have focused requirements for these capabilities and therefore hiring and training practices focus on acquiring those skillsets. OSINT, for many targets, has similar language needs, but every analyst cannot be language proficient even if every analyst is inherently an OSINT collector.

Regional and Cultural Expertise: The ability to identify good OSINT and utilize it for details or context in all-source analysis typically relies on an appreciation for the cultural context surrounding that open source. Similar to language requirements, however, many all-source analysts are not experts in their particular region. Partly, this is due to the massive expansion of the intelligence community following September 11. Though specific numbers of personnel are typically classified, the hiring efforts after 9/11 led to nearly half of IC analysts in 2013 having fewer than six years of experience.[50] Many of these hires have been young, energetic, and straight out of school, and the IC has focused on training them in terrorist network targeting, analytical tradecraft, IC common practices, collaboration, etc.; all the qualities of a good, general all-source analyst. However, their lack of regional expertise beyond individual study and on-the-job training can lead to a lack of cultural context. Anecdotally, analysts unfamiliar with the

culture of their target region are also likely to be unfamiliar with the types of open sources, such as social media networks or unofficial or unestablished media sources. Newer analysts are also less likely to be familiar with established academic research, journals, experts, etc. to enable a deeper understanding of a particular issue.

Costs: PAI, ironically, is not always free. In many cases, companies charge fees for access to their extensive, open-source databases. In the case of defense intelligence, Jane's offers a good example. Jane's is a British publishing company with a heavy focus on defense-related issues that advertises itself on its website as a "leading global open source intelligence agency."[51] In one Canadian Defence Intelligence assessment, access to Jane's and an additional 40 similar databases costs approximately $3.4 million per year.[52]

Policy Restrictions: Numerous policies restrict the abilities of analysts to gain access to PAI, but the two most prominent involve technical/operational security (OPSEC) and restrictions on intelligence collection against U.S. citizens. OSINT experts at Marine Corps Intelligence Activity, for example, have difficulty gaining access to the internet through Marine Corps systems due to concerns over network vulnerability. Potential solutions for this, including carefully controlled automated open source collection software that pushes PAI to analysts over closed systems, run into problems of inadvertent collection on U.S. persons and companies.[53]

Culture: Culture, of both policymakers and the IC, probably has the greatest impact on establishing OSINT as the first resort. As former CIA official Arthur Hulnick noted in 1999, "Policy officials are rarely interested in unclassified analysis. They see it as no better than the

New York Times."[54] Informal discussions with analysts around the intelligence community suggest this attitude has not changed. Unless requested, if an analyst were to write an entirely unclassified report, his chain of command likely would not publish the report or would request additional classified sources, regardless of whether or not the product satisfies the requirement. This culture stems largely from an attitude of self-preservation and justification for resources. Similar to the fundamental question of intelligence vs. information, a policymaker provided with an unclassified report from an intelligence agency might question what value the IC provides or why the IC requires so much money and resources if the policymaker can get the same answers from the private sector. This is not an issue that can be easily solved, but thoughtful application of OSINT would serve to demonstrate benefits to policymakers and senior IC officials.

Open Source Enterprise Goals

With the establishment of the NOSE in 2006, the DNI signaled a renewed focus to address the challenges of OSINT and establish its place within the broader IC. The NOSE's original mission was to ensure the "active and efficient use of open source intelligence, information, and analysis by the IC through the establishment and maintenance of an effective, reliable, and collaborative capability that provides maximum availability of open source information to all consumers, optimizes resource utilization, and establishes effective burden sharing."[55] Subsequent strategic plans from both the NOSC and DOSC demonstrate continued refinement of that original goal (see Table 1).[56] [57] [58] [59]

NOSE Strategic Plan 2006	NOSE Strategic Plan 2009	DoD PAI Strategic Plan 2016
1. Utilize OSINT as a source of first resort.	1. Universal, cross-domain (Top Secret, Secret, Unclassified) access	1. Lead and manage an efficient and effective integrated [open source] enterprise.
2. Establish a guild of OSINT experts, including universal training and outreach to the private/academic sector.	2. Integrated mission management and impact	2. Provision and enable PAI for the Defense Intelligence Enterprise.
3. Acquire global OSINT input from the widest available resources, including capabilities and requirements management.	3. Proliferation of open source expertise	3. Develop and sustain a skilled workforce.
4. Build a single OSINT information technology architecture.	4. Open Source Enterprise governance	
5. Establish a small, dedicated OSINT working group for innovation and integration.		

Table 1. Open Source Strategic Plans

Applied Solutions

Today's Defense Intelligence Enterprise offers the most illustrative cross-section of the U.S. IC to demonstrate potential solutions for OSINT. With the broadest customer base in the I.C., defense intelligence spans the spectrum of strategic, operational, and tactical intelligence while engaged in extensive collaboration with both foreign partners and domestic law enforcement agencies. As demonstrated in Figure 1, the complexities of OSINT require solutions across a broad spectrum of issues:[60]

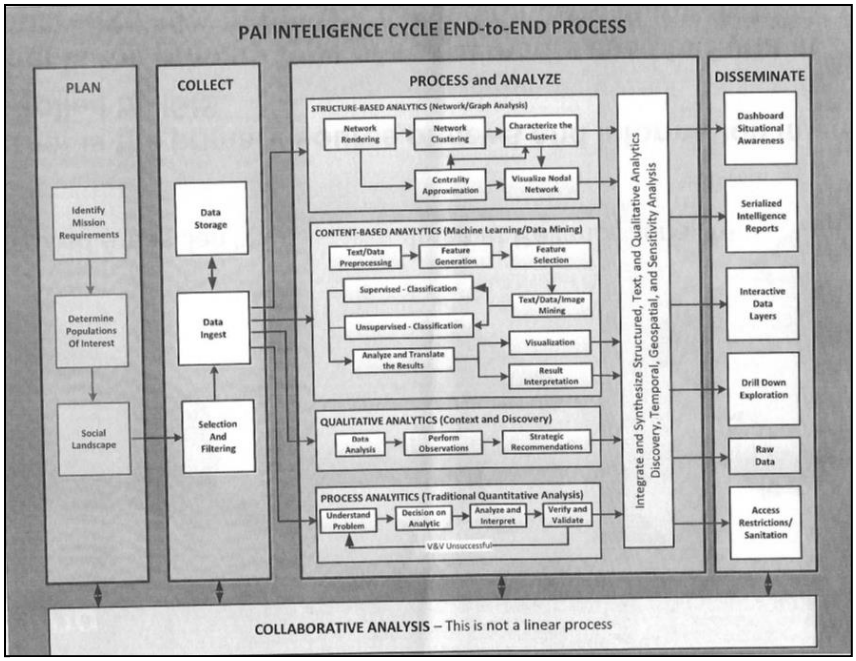

Figure 1: PAI Cycle

DIA, as the DoD lead component for OSINT, is engaged in several initiatives aimed at addressing challenges that fit effectively three key focus areas in the strategic plan: integration, technology, and expertise.[61]

Integration

Open Source Cells: Combatant command J2s are establishing open source cells designed to address CCMD OSINT requirements. The Marine Corps Intelligence Activity proposed a similar concept in 2016 entitled the "PAI Collaborative Laboratory". The concept involved teams of functional and regional experts working alongside data scientists and other information experts on a particular problem set. Each team (or laboratory) would involve a core staff amplified by joint and interagency detailees with the ability to contract to private sector experts on a regular basis. On a broad scale, the vision would include international partnerships with linked global cells to achieve time dominance in a constantly shifting discipline.[62] The initiative has yet to be approved on a wide scale.

Technology

Machine Translation: Anecdotally, DIA analysts have indicated machine translation, such as Google Translate, has allowed them to overcome a lack of language expertise. The specificity and technical jargon of defense intelligence, however, limits the utility of machine translation.

Secure Unclassified Networks: To overcome concerns over attribution and OPSEC, some organizations, such as the Marine Corps, have developed or acquired secure networks specifically to collect OSINT utilizing automated tools and specially designed user interfaces.

Automated Collection Tools: To keep pace with the increasingly vast quantities of information (often termed as big data), the DIE is turning to automated tools to pull relevant information to then be analyzed by human analysts. As noted, MCIA, has acquired several different tools on a secure unclassified network to consolidate and visualize PAI. Automation, however, has challenges with the potential for collecting on U.S. persons and inability to merge information from separate, proprietary software.[63]

Expertise

Training: DIA currently has a draft training plan awaiting approval by the DOSC that will be implemented within DIA's Academy for Defense Intelligence (ADI). As with much of OSINT training within the IC, however, it is not mandatory and is focused primarily on developing OSINT experts as opposed to providing training across the broad scope of all-source analysts.

Open Source Collectors: DIA is considering establishing a new open source collector position, similar to those already employed at the CIA, that would aim to hire qualified open source experts to address the current gaps in all-source analyst training and expertise.[64] [65]

Solutions

Potential OSINT solutions for the IC, and the Defense Intelligence Enterprise specifically, fall onto a spectrum. On one end are systemic approaches that would restructure the IC towards today's information and threat environments, much as the establishment of ODNI did for the interagency process. These approaches would be effective but difficult to achieve. On the other end are individual, tailored solutions that can be applied within the current structure of the IC, many of which are outlined above. These approaches are more easily achieved but do not address the underlying disparity between the problem and the solutions.

Systemic Solutions

Most arguments for complete restructuring come from outside the IC, including academics, lawmakers, or even former IC professionals. Robert Steele, former Deputy Director of MCIA and a strong advocate for open and public information dissemination, championed a piece of legislation entitled "The Smart Nation Act" proposed by Congressman Rob Simmons in 2006. In his proposed legislation, Rep. Simmons argued for:

- An Open Source Intelligence Program to manage OSINT across the U.S. IC
- A centralized raw unclassified processing center and a digitization facility
- A Congressional Public Intelligence Office to provide tailored OSINT to Congress
- An Open Source Agency (OSA) to provide open source information to the public free of

charge

- An Office of Information Sharing Treaties and Agreements within the Department of State to facilitate arrangements with other countries
- An Open Source Field Activity within the Department of Defense to meet all DoD OSINT requirements and to push OSA information to classified intelligence systems
- Fifty state-based Community Intelligence Centers run by the National Guard

Academic William Lahneman, recognizing the need for the IC to maintain its traditional roles of classified collection and analysis, splits the responsibilities of the IC between this traditional role and the necessity to expand OSINT. He proposes:[66]

- Traditional IC agencies remain as is, focused on their traditional role analyzing hard-target adversaries.
- An Office of Strategic Information (OSI) outside of the IC to conduct adaptive interpretations at the unclassified levels
- U.S. IC incorporates OSI reports into its classified analysis, conducting its own adaptive interpretations in an Integrated Information Analysis Center (IIAC)
- Split collection away from all-source agencies, in order to functionalize collection stovepipes, as opposed to agency stovepipes
- Maintain a sharing skillset within the IIAC

Targeted Solutions

More targeted solutions aim to address specific challenges. Most of the actions being taken by the NOSC and DOSC fall into this category, as they aim to improve OSINT within the

current system. In addition to the actions outlined above, the below proposals offer a laundry list of initiatives that could be enacted at all levels of the IC and DIE to continue marginal OSINT improvements:

- *Allied burden sharing of OSINT*. OSINT sharing is already an inherent part of any international all-source intelligence burden sharing relationship. The importance of regional and cultural expertise, however, suggests that the U.S. IC could accept greater risk within its own intelligence processes by outsourcing its OSINT analysis to regional partners. The ability to share OSINT could also expand sharing to non-traditional partners.
- *Joint official and private sector NIEs*. NIEs currently include summaries of outside experts' views.[67] A more bottom-up, integrated approach to NIEs, however, could encourage analysts at the working level to solicit outside input at the outset on the IC's most critical questions.
- *PAI Communities of Interest (COI).* The IC already provides several applications that encourage collaboration between analysts, such as Intellipedia and A-Space.[68] Increased focus on OSINT within these COIs, however, would enable analysts to crowdsource trusted PAI, particularly new analysts with limited expertise.
- *Mandatory OSINT Training*. OSINT training has been making great strides within the last few years due to efforts by the NOSC and DOSC. This training, however, is voluntary and provided largely to OSINT professionals. Mandatory training, such as onboarding training at DIA for example, provides only a cursory overview of OSINT. Given its broad applicability, in-depth OSINT training should be mandatory for all-source analysts.

- *Language Hiring and Training*. Given that every all-source analyst is inherently an OSINT collector, language and OSINT requirements for all-source analyst positions should be closely aligned in order to improve OSINT capabilities across the enterprise at the working level.

Recommendation

As demonstrated, OSINT context is necessary at all stages of the intelligence cycle and at the most basic levels of analysis. Widespread recognition at the highest levels has enabled leadership within the OSINT community to make considerable progress towards improvements throughout the IC. As identified in a DIA presentation to a PAI Synch Conference in September 2016 recognized, "After a decade of fits and starts—a foundation is beginning to take shape."[69] Tangible progress at the working level is limited, however.

Systemic solutions, such as that offered by William Lahneman, offer comprehensive reform designed to improve OSINT at all levels. Lahneman's proposal specifically serves to maintain the IC's traditional role while shortening the cycle for more "adaptive interpretations." Independent OSINT and classified IC analyses that require synthesis and deconfliction at the policy level, however, are untenable. Senior officials share the sentiment; according to Mr. Andy Roberts, DOSC Chair, "There is no appetite for an independent OSINT agency." The most likely solutions, therefore, must work within the current confines of the IC structure and processes but infuse the spirit of reform and "adaptive interpretation" into both top-down and bottom-up targeted solutions.

Conclusion

The U.S. IC and policymakers understand the importance of open source information, but the IC has not adapted its culture and practices to address it. A continued focus on traditional, secret intelligence disciplines hampers the IC's ability to fully adjust to today's information and threat environments. Absent adjustments, a high proportion of U.S. intelligence analysis will rely on increasing amounts of noise. Traditional, secret intelligence disciplines cannot keep up with the vast amounts of information or address the preponderance of threats the U.S. faces today. Rigorous OSINT and changes to processes and training necessary to provide it will be critical if the IC is to continue its primary function of preventing strategic surprise to U.S. interests.

---

[1] Alvin Toffler, *Future Shock* (New York: Random House, 1970), 31.
[2] Richard N. Haass, *Intervention: The Use of American Military Force in the Post-Cold War World* (Washington D.C.: Brookings Institute Press, 1998), ProQuest Ebook Central, 2.
[3] Joint Military Intelligence Training Center. *Open Source Intelligence: Professional Handbook*. October 1996, 6.
[4] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), 387.
[5] "Information revolution," *Dictionary.com's 21st Century Lexicon*. Dictionary.com, LLC, accessed: April 2, 2018, http://www.dictionary.com/browse/information-revolution.
[6] ODNI, "What is Intelligence?" *Office of Director of National Intelligence*, accessed January 18, 2018, https://www.odni.gov/index.php/what-we-do/what-is-intelligence.
[7] Dr. Melissa Burn (Chief, Marine Corps Intelligence Activity OSINT), discussion with author, January 25, 2018.
[8] *Intelligence Reform and Terrorism Prevention Act of 2004*, PL 108-458 (December 17, 2004): STAT. 3683.
[9] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States* (Washington, DC: Government Printing Office, 2005), 378-380.
[10] Vee Harrington, "Intelligence Reform Brings New Opportunities for Info Pros," *Information Outlook* 12:3 (March 2008), 12-13.
[11] US Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, January 2018), 2-3.
[12] ODNI, "What is Intelligence?" *Office of Director of National Intelligence*, accessed January 18, 2018, https://www.odni.gov/index.php/what-we-do/what-is-intelligence.
[13] Joint Military Intelligence Training Center. *Open Source Intelligence: Professional Handbook*. October 1996, 24.
[14] Defense Intelligence Agency, *Expeditionary Open Source Intelligence Handbook* (Washington DC: Academy for Defense Intelligence, 2018), 6.
[15] Olga Khazan, "Gentlemen Reading Each Others' Mail: A Brief History of Diplomatic Spying," *The Atlantic*, June 17, 2013, https://www.theatlantic.com/international/archive/2013/06/gentlemen-reading-each-others-mail-a-brief-history-of-diplomatic-spying/276940/.
[16] Michael Warner, "The Creation of the Central Intelligence Group", *Studies in Strategic Intelligence* Vol. 39, No. 5 (2007): 112, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a13p.pdf.
[17] Ibid, 114.
[18] Mark Lowenthal, *Intelligence: From Secrets To Policy (Sixth Edition)* (Washington, DC: CQ Press, 2015), 2-5.
[19] Mats Berdal, "The New Wars Thesis Revisited" in *The Changing Character of War*, ed. Hew Strachan and Sibylle Scheipers, 109-138 (New York: Oxford University Press, 2014), 110.
[20] Strategic Studies Institute, *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: Strategic Studies Institute, June 2016), 5.
[21] "Intelligence Reform: Challenging the Conventional Wisdom Part 1," YouTube video, July 15, 2014, 14:07, https://www.youtube.com/watch?v=f02AEU3qpdY.

[22] US Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, January 2018), 2.
[23] James Garamone, "Dunford Details Implications of Today's Threats on Tomorrow's Strategy," DoD News, https://www.defense.gov/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy/ (August 23, 2016).
[24] Mark Lowenthal, *Intelligence: From Secrets To Policy (Sixth Edition)* (Washington, DC: CQ Press, 2015), 2-3.
[25] Ariel Levite, *Intelligence and Strategic Surprises* (New York: Columbia University Press, 1987), 1.
[26] Ibid, 1-3.
[27] M.G. Siegler, "Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003," *Tech Crunch*, August 4, 2010, https://techcrunch.com/2010/08/04/schmidt-data/.
[28] IBM, "Bringing big data to the enterprise," accessed February 2, 2018, https://www-01.ibm.com/software/in/data/bigdata/.
[29] Harold Lasswell, "The Structure and Function of Communication in Society," in *The Communication of Ideas,* ed. L. Bryson (New York: Harper and Row, 1948), 37.
[30] Anthony Olcott, *Open Source Intelligence in a Networked World* (London: Continuum International Publishing Group, 2012), 12-13.
[31] Ibid, 178.
[32] Ibid, 200.
[33] Ibid, 178.
[34] Ibid, 8.
[35] Ibid, 10.
[36] Ibid, 11.
[37] Joseph E. Roop, *Foreign Broadcast Information Service, History Part I: 1941-1947* (Langley, VA: Center for the Study of Intelligence, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/foreign-broadcast-information-service/5-FBIS-Intergovernmental-Relations.pdf, 121, Jan 16
[38] Anthony Olcott, *Open Source Intelligence in a Networked World* (London: Continuum International Publishing Group, 2012), 12-13.
[39] Ibid, 15.
[40] Ibid, 30-31.
[41] Ibid, 16.
[42] Joseph E. Roop, *Foreign Broadcast Information Service, History Part I: 1941-1947* (Langley, VA: Center for the Study of Intelligence, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/foreign-broadcast-information-service/5-FBIS-Intergovernmental-Relations.pdf, 299-303, Jan 16
[43] National Security Act of 1947, 253 U.S.C. § 102
[44] Central Intelligence Agency, "Establishment of the DNI Open Source Center," https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr11082005.html, November 8, 2005.
[45] Steven Aftergood, "Open Source Center (OSC) Becomes Open Source Enterprise (OSE)," *Federation of American Scientists*, posted October 28, 2005, https://fas.org/blogs/secrecy/2015/10/osc-ose/.
[46] Vee Herrington, "Intelligence Reform Brings New Opportunities for Info Pros," *Information Outlook* 12:3 (March 2008), 12-13.
[47] US Director of National Intelligence, *National Open Source Enterprise*, Intelligence Community Directive 301, January 11, 2006.
[48] US Department of Defense, *Open Source Intelligene (OSINT)*, Instruction 3115.12, August 24, 2010, 2.
[49] Steven Aftergood, "Open Source Center (OSC) Becomes Open Source Enterprise (OSE)," *Federation of American Scientists*, posted October 28, 2005, https://fas.org/blogs/secrecy/2015/10/osc-ose/.
[50] Mark Lowenthal, *Intelligence: From Secrets To Policy* (Sixth Edition). (Washington, DC: CQ Press, 2015), 195.
[51] IHS Markit, "Jane's – Intelligence that matters," https://ihsmarkit.com/videos/janes-intelligence-matters.html.
[52] Lesley Hoermann, *OSINT Operational Support* (Canadian Forces Intelligence Group, May 31, 2017), Powerpoint presentation, 7.
[53] Dr. Melissa Burn (Chief, Marine Corps Intelligence Activity OSINT), discussion with author, January 25, 2018.
[54] Arthur Hulnick, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-first Century* (Westport, CT: Greenwood Publishing Group, 1999), 8.
[55] Office of Director of National Intelligence, *National Open Source Enterprise,* Intelligence Community Directive 301, January 11, 2006, 2.
[56] Office of Director of National Intelligence, *National Open Source Enterprise* (Washington D.C., 2006), 8-12, https://fas.org/irp/dni/osc/nose.pdf.

[57] Vee Herrington, "Intelligence Reform Brings New Opportunities for Info Pros," *Information Outlook* 12:3 (March 2008), 12-13.
[58] Office of National Director of Intelligence, *National Open Source Strategic Action Plan* (Washington D.C., 2009), 7, https://fas.org/irp/dni/osc/nossap.pdf.
[59] Defense Intelligence Agency, *DoD Intelligence PAI Strategic Action Plan* (PAI Senior Synchronization Conference, September 29, 2016), Powerpoint presentation, 1.
[60] Ian McCulloh, *Mobilizing for PAI Utilization* (PAI Senior Synchronization Conference, September 29, 2016), Powerpoint presentation, 7.
[61] Mr. Andrew Roberts (Chairman, Defense Open Source Council), discussion with author, November 20, 2017.
[62] Dr. Melissa Burn (Chief, Marine Corps Intelligence Activity OSINT), discussion with author, January 25, 2018.
[63] Dr. Melissa Burn (Chief, Marine Corps Intelligence Activity OSINT), discussion with author, January 25, 2018.
[64] Mr. Andrew Roberts (Chairman, Defense Open Source Council), discussion with author, November 20, 2017.
[65] Central Intelligence Agency, "Open Source Collection Officer Career Opportunity," last modified February 23, 2018, https://www.cia.gov/careers/opportunities/analytical/open-source-officer-foreign-media-analyst.html.
[66] William J. Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs* (Lanham, MD: Scarecrow Press, 2011), ProQuest Ebook Central, 131-146.
[67] Loch K. Johnson, ed. *Strategic Intelligence, Volume 2: The Intelligence Cycle* (Westport, CT: Praeger Security International, 2007), 319.
[68] Massimo Calabresi, "Wikipedia for Spies: The CIA Discovers Web 2.0," *TIME Magazine*, April 8, 2009, http://content.time.com/time/nation/article/0,8599,1890084,00.html.
[69] Defense Intelligence Agency, *Strategic Plan and Priorities* (PAI Senior Synchronization Conference, September 29, 2016), 3.

Bibliography

Boot, Max. *War Made New: Weapons, Warriors, and the Making of the Modern World*. London: Penguin Books, 2007.

Calabresi, Massimo. "Wikipedia for Spies: The CIA Discovers Web 2.0." *TIME Magazine*, April 8, 2009. http://content.time.com/time/nation/article/0,8599,1890084,00.html.

Central Intelligence Agency. "From Pearl Harbor to the Digital Age: Open Source Enterprise Celebrates 75th Anniversary," last modified December 12, 2016, https://www.cia.gov/news-information/featured-story-archive/2016-featured-story-archive/ose-pearl-harbor-to-digital-age.html.

Freier, Nathan. "Outplayed: Regaining Strategic Initiative in the Gray Zone." Strategic Studies Institute, June 2016.

Gonzalez, Gabriella V. "OSINT as an NMOS." *Marine Corps Gazette* 101, no. 9 (09, 2017): 49-52. https://search-proquest-com.lomc.idm.oclc.org/docview/1934947770?accountid=14746.

Haass, Richard N. *Intervention: The Use of American Military Force in the Post-Cold War World*. Washington D.C.: Brookings Institute Press, 1998. ProQuest Ebook Central.

Herrington, Vee. "Intelligence Reform Brings New Opportunities for Info Pros." *Information Outlook* 12, no. 3 (Mar 1, 2008): 10. https://search.proquest.com/docview/197379471.

Hoermann, Lesley. *OSINT Operational Support.* Powerpoint presentation. Canadian Forces Intelligence Group, May 31, 2017.

Hoffmann, Frank G. "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War." In *2016 Index of U.S. Military Strength*. Heritage Foundation, https://index.heritage.org/military/2016/essays/contemporary-spectrum-of-conflict/, 2016.

Hulnick, Arthur. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-first Century*. Westport, CT: Greenwood Publishing Group, 1999.

Joint Military Intelligence Training Center. *Open Source Intelligence: Professional Handbook.* October 1996.

Johnson, Loch K., ed. *Strategic Intelligence, Volume 2: The Intelligence Cycle.* Westport, CT: Praeger Security International, 2007.

Lahneman, William J. *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*. Lanham, MD: Scarecrow Press, 2011. ProQuest Ebook Central.

Laqueur, Walter. *The Uses and Limits of Intelligence*. New Brunswick, NJ: Transaction Publishers, 1993.

Levite, Ariel. *Intelligence and Strategic Surprises*. New York: Columbia University Press, 1987.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Sixth Edition. ed. Los Angeles: CQ Press, 2015.

McCulloh, Ian. *Mobilizing for PAI Utilization.* Powerpoint presentation. PAI Senior Synchronization Conference, September 29, 2016.

Olcott, Anthony. *Open Source Intelligence in a Networked World*. New York: Continuum International Publishing Group, 2012.

Roop, Joseph. "Foreign Broadcast Information Service: History, Part I." CIA, 2009.

Steele, Robert David. *The Smart Nation Act: Public Intelligence in the Public Interest*. Oakton, Va.: OSS International Press, 2006.

Steele, Robert David, and OSS International Press. *Information Operations: All Information, All Languages, All the Time*. Oakton, Va.: OSS, 2006.

Treverton, Gregory F. *Reshaping National Intelligence for an Age of Information*. Cambridge, UK: Cambridge University Press, 2003.

US Department of Defense. *Open Source Intelligence (OSINT)*. Instruction 3115.12, August 24, 2010.

US Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America.* Washington, DC: Office of the Secretary of Defense, January 2018.

US Defense Intelligence Agency. *DoD Intelligence PAI Strategic Action Plan.* Powerpoint presentation. PAI Senior Synchronization Conference, September 29, 2016.

US Defense Intelligence Agency. *Expeditionary Open Source Intelligence Handbook.* Washington DC: Academy for Defense Intelligence, 2018.

US Office of Director of National Intelligence. *National Open Source Enterprise*. Intelligence Community Directive 301. July 11, 2006. https://fas.org/irp/dni/icd/icd-301.pdf.

US Office of Director of National Intelligence. *National Open Source Enterprise.* Washington D.C., 2006. https://fas.org/irp/dni/osc/nose.pdf.

US Office of National Director of Intelligence. *National Open Source Strategic Action Plan.* Washington D.C., 2009. https://fas.org/irp/dni/osc/nossap.pdf.

Toffler, Alvin. *Future Shock.* New York: Random House, 1970.

Van Creveld, Martin. *Command in War.* Cambridge, MA: Harvard University Press, 1985.

Warner, Michael. "The Creation of the Central Intelligence Group." In *Studies in Intelligence*. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a13p.pdf. Accessed on Jan 17.