Fall 2014

Why haven't technologies fixed open source intelligence?

Timothy Sparks
James Madison University

Why Haven’t Technologies Fixed Open Source Intelligence?

Timothy D. Sparks

A thesis submitted to the Graduate Faculty of

JAMES MADISON UNIVERSITY

In

Partial Fulfillment of the Requirements

for the degree of

Master of Science

Integrated Science & Technology

December 2014

Acknowledgements

What a journey! I would like to acknowledge some folks who inspired me to complete this program. First, Dr. Barbara Gabriel, the former graduate director of the Integrated Science and Technology program. Dr. Gabriel convinced me to enroll in the program and ultimately helped develop this thesis. She encouraged me to persevere and complete it before her retirement, however it has taken me longer than expected. I owe gratitude and thanks to my thesis committee: Dr. Jeffrey Tang, Chair, Dr. Tim Walton, and David McGraw, J.D. Their guidance, time, and encouragement during this process kept me on track and focused to the best of their abilities. To Dr. Ming Ivory, thanks for guiding me through the last several years, I truly appreciate your efforts. In addition, there were many outstanding professors who taught me many challenging subjects and new problem solving skills. Specifically, I'd like to thank Dr. Bob Kolvoord, Dr. Michael Deaton, and Dr. George Baker for your enthusiasm and support. Finally, I'd like to thank all of the professors, staff, and fellow graduate students in the MSISAT program and The Graduate School. I'll always look back on this program and at James Madison University with fondness.

To my wife Sheila – I have finally tied a "bow" on it. Thanks for your support, encouragement, love and patience over the years. On to more exciting times! To my kids Morgan and Collin, I dedicate this effort. It takes hard work, perseverance, and determination to realize your goals; it's worth your time to set lofty goals and work hard to achieve them. The rewards in life await you.

Table of Contents

List of Tables

List of Figures

Abstract

The Intelligence Community (IC) reached consensus after 9/11/2001 on the importance of Open Source Intelligence (OSINT) due to the changing nature of the global threat environment, the information explosion, and the changing intelligence requirements of the IC. Voluminous amounts of information, much of it with potential application for use in intelligence operations, continue to challenge IC intelligence analysts' capabilities to harness, and effectively use in finished all-source intelligence production. Government reform commissions, senior IC officials, along with OSINT and technology advocates, have all espoused the growing importance of OSINT, and have outlined many ways in which the IC should improve including through improved OSINT training and expertise, along with the application of technologies and tools to assist IC analysts to perform the OSINT mission. This thesis examines how OSINT became important again after the events of 9/11, and the systematic efforts to institutionalize OSINT within the IC. This thesis examines the envisioned state of OSINT as published in the 2006 National Open Source Enterprise OSINT vision, that OSINT would be used as the "Source of First Resort", and examines past IC efforts to implement technological solutions to make OSINT better for IC analysts. This examination attempts to answer the simple question of why haven't technologies fixed OSINT yet? The thesis outlines many of the IC cultural challenges and limitations of the IC, as reflected in the literature, and personal observations of IC challenges that have inhibited OSINT, or may do so in the future. The thesis concludes by highlighting where OSINT has been and the unclear status of OSINT in the future IC. It is unknown whether OSINT will ever reach its full potential within the IC, or if on-going OSINT initiatives and reform efforts will repeat past trends.

Further research may be required to understand future IC OSINT initiatives and how well OSINT fares in the coming years.

Keywords: Open Source Intelligence, OSINT, Intelligence Community, Reform, National Open Source Enterprise

CHAPTER 1

INTRODUCTION

"The open-source world represents a major challenge to the U.S. Intelligence Community, which is, in addition to being an espionage service, is one of the world's biggest information-based businesses. The open-source challenge is a longstanding high priority for us, and our response to it is very much a dynamic work in progress." (National Intelligence Council Chairman, John C. Gannon, 6 October 2000)

Throughout its existence, United States (U.S.) Intelligence Community (IC) officials have been grappling with how to fully exploit information available from publicly available sources, such as from the press and other published information. Officials within the U.S. IC have made recommendations in how to structure open source intelligence (OSINT) efforts amongst its member agencies. The IC has attempted to establish OSINT as a bon-a-fide intelligence discipline, institutionalize its practices, and promote greater use within the IC. Attempts have been made to change prevailing attitudes on the merits and value of OSINT, with some measurable success. With the rise of 'big data' in recent years, there has been a lot of attention paid to a myriad of possible technological solutions. Information technology advances over the last several decades have impacted the methods of the IC to harvest and utilize OSINT in ways never imagined over 60 years ago during the formation of the IC.

Thesis Statement

This thesis will examine how the importance of OSINT has grown over the last sixty years within the IC, during times of major global threat changes, challenges, and throughout the information revolution and great technological innovations, especially in the aftermath of intelligence "failures" of 9/11/2001.

OSINT reforms have often been recommended throughout the history of the IC from a variety of reform commissions, and independent commission recommendations. The changing nature of global threats and growth in the number of intelligence targets has increased the amount of information required to conduct more informed, effective intelligence analysis. The globalization of information has also resulted in an increase in the amount of available sources of information, from both classified and open sources, to be considered by the intelligence analyst and has created an information overload that is likely to only worsen over time. Mid-2000's reform efforts for OSINT included naming a national-level advocate, publishing of the 2006 National Open Source Enterprise (NOSE) OSINT vision (Jardines, 2006), and issuing an IC Intelligence Community Directive (ICD) that established OSINT's position within the IC. OSINT as a discrete topic, worthy of individual attention, seemed to reach its height of popularity in 2008.

Many have recommended solutions for how OSINT should be produced, structured, and emphasized more effectively within the IC. This thesis examines one of the key recommendations to improve how OSINT is performed, through the better adoption and implementation of tools and technologies. This examination sets out to answer the simple question of why technologies haven't fixed OSINT in the IC, despite its long noted importance within the IC. This paper also examines IC system limitations and constraints that may keep the IC from realizing the potential benefits of an improved use of OSINT. This thesis concludes with an examination of what happened to the 2006 NOSE OSINT vision, and outlines the potential future for OSINT within the IC.

OSINT in the Post 9/11 IC

Nearly 10 years ago and on the heels of two major intelligence reforms calling for the increased use of OSINT by the IC, David Rothkopf (2005), then Chief Executive Officer (CEO) of Intellibridge and former Deputy Under Secretary of Commerce for International Trade Policy and Development, wrote a provocative essay on the benefits of technology to U.S. Intelligence entitled “Technology Can Fix U.S. Intelligence”. The article claimed that the measures called for in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA) bill evaded real reform efforts. He referred to the long running issue of OSINT as one that remained unsettled, and suggested that IC should solve this issue once and for all, which would then free up monies for more advanced technologies. Rothkopf asserted that “If the government stopped spending billions producing what was already available for free or at low cost on the Web, then it could devote more money to the new technologies that will truly transform intelligence.” He related that a senior military commander once told him “…that perhaps 95 percent of what is now deemed secret is available via open sources, thanks to the Internet” (Rothkopf, 2005, p.34). Rothkopf also noted that there are problems within the current system of intelligence, that “Unbelievably, many in the national-security community don’t have full access to the Web…” (Rothkopf, 2005, p. 34).

The IC did make an effort to actively promote OSINT within the Department of Defense (DoD) and the IC. The Director of National Intelligence (DNI) Open Source Center (OSC) held its first-ever meeting with DoD components and Combatant Commands on issues surrounding OSINT in 2005 (Peak, 2005). This conference set out to discuss key issues such as managing OSINT requirements, information sharing and dissemination practices, how to better use subject-matter experts, and also discussed technology enablers aimed at improving the ways in which OSINT was produced. The goal was for the OSC to work with the DoD to de-conflict strategies and reduce redundancies in the production of OSINT.

Two years later, and while celebrating the IC's 60th Anniversary, the DNI hosted the first ever IC sponsored conference on OSINT and featured discussions on issues in a public forum like never before. Then DNI Admiral J. Mike McConnell (ret.), the keynote speaker for the conference, related that the vast amount of open source information, some 600,000 terabits passing through the internet on a daily basis presented the IC with a challenge to "…have it available, to sort it out, to be able to touch it, to be able to examine it, to be able to have it useful in the context of the problems we're attempting to work".   McConnell also noted that "The other thing that's missing are the tools. Currently our systems are, for the most part, closed. It's difficult for some of our analysts to have access to the web" (McConnell, 2007).

Ms. Sabre Horn, then Office of the DNI (ODNI) Senior Advisor for Open Source, introduced the newly appointed Assistant Deputy Director for National Intelligence for Open Source (ADDNI/OS), Mr. Eliot Jardines. Ms. Horn related that Jardines' vision in transforming open source as the "source of first resort" will ensure "…that open source will no longer be what we've ever known it to be before" (Jardines, 2007). Jardines further defined his vision of OSINT during his remarks:

> Open sources should be the precursor to all clandestine and technical collection and better employed to support all collection and analysis activities. In other

> words, we must leverage open sources, not only to answer immediate questions but to preserve and enable classified capabilities. (Jardines, 2007)

Patience Wait, a staff member of Government Computer News, also captured Jardines sentiments on OSINT shortly after he assumed his new position. Jardines stated that "Getting the [intelligence Community] (sic) to accept open source as the source of first resort is my number one goal" (Wait, 2006).

These two OSINT forums, along with the establishment and appointment of Jardines as the nation's highest ranking advocate for OSINT had pushed discussions on the importance of OSINT into a public forum like at no other time throughout the existence of the IC. Perhaps fitting for long-time OSINT advocates, the IC had finally recognized that they must build a better way of conducting the business of OSINT.

The 2006 National Open Source Enterprise OSINT Vision

In 2006, the DNI established the NOSE, an IC-wide effort aimed at ensuring that OSINT was better positioned and utilized within the IC, with Jardines as its leader. The NOSE formulated and published its vision for OSINT the same year (Jardines, 2006). This visionary outline was the first attempt to establish a formal, institutionally directed path for OSINT within the IC. Jardines proclaimed in the opening message of the publication that "The richness of the information age and the pace of technological innovation offer us tremendous opportunities; what is unknowable now may well be attainable in the future." He would elaborate further that "The task before us is to develop the expertise, tools, and culture of sharing to best harvest the information we need. Ignoring open sources is no longer an option; they must be viewed as the source of first resort" (Jardines, 2006, p. 3). The NOSE outlined 5 goals for OSINT. Table 1 below summarizes the 5 goals contained in the 2006 NOSE OSINT Vision.

Table 1

Goals Outlined in the 2006 NOSE OSINT Brochure

Goal	Title	Objective	Description
One	Source of First Resort	Open source is the source of first resort for all disciplines and the precursor for clandestine and technical collection.	OSINT fully exploited as the source of first resort; Effect Cultural Change within IC; National Open Source Committee drives the future for OSINT within the IC
Two	Guild	Our people are empowered by a guild of experts who champion the use of open sources, by universal training in open source exploitation, and by embedding open sources in the work of all disciplines.	Establishes OSC as Center of Excellence; Open Source embedded as a universal competency within IC; Open source part of all training
Three	Global Input	Global input ensures the broadest range of information with relevant sourcing background is accessible to all consumers.	Build inventory of existing OSINT capabilities; Create a single open source requirements management system; Global input from widest range of sources possible
Four	Single Architecture	A single open source architecture provides optimum access to information - acquired once and shared with all.	A single open source architecture facilitates integration of open sources in all intelligence disciplines; Open Source Architecture fosters collaboration; Content is available to broadest range of consumers possible
Five	Open Source Works	A robust Skunk Works®-like capability anticipates and capitalizes on emerging opportunities driving innovation in tradecraft, analysis, and technology.	Open-Source Works fosters and leverages a loose confederation of related public and private activities; Furthers National Intelligence Strategy objectives by integrating open source with other intelligence disciplines; Board of Advisors stimulates innovation; Fuels competitive analysis
		Adapted From: Jardines, 2006, NOSE OSINT Brochure	

OSINT within the IC was clearly a high priority in 2007. Newly established IC leadership had deliberately set out to finally address long noted OSINT deficiencies along with a prescription for how to increase the use of OSINT within the IC. The DNI had established the ADDNI/OS, published the 2006 NOSE OSINT vision, and had formally issued ICD 301 which prescribed the conduct of OSINT activities within the IC. The IC seemed on the verge of finally settling and addressing decades of recommended OSINT reforms.

The story of OSINT in 2014 appears to be an unfinished story. The IC has largely failed to fully institutionalize OSINT. The 2006 NOSE OSINT vision has long been replaced, and a lot of the ideas espoused in the vision remain a past memory. The IC no longer has an ICD that prescribes the direction of OSINT. The IC advocate for OSINT has been moved back to an existing collection agency. Many OSINT advocates wonder what happened to IC initiatives for OSINT from nearly a decade ago.

Defining OSINT & OSINF

Before proceeding, there are some key terms that must be defined. The first is open source information (OSINF). OSINF has been defined as any information within the public domain. Some examples include books, magazine articles, information found on the web, literature, the media, and so on. OSINF remains information until it is collected and processed for intelligence work (Lowenthal, 1999). This information is commonly referred to hereafter as vast amounts of OSINF, or publicly available information.

The most common term used throughout this discussion is OSINT. The definition of OSINT comes from the National Defense Authorization Act for Fiscal Year 2006 (NDAA, 2006), which later was copied for the IC definition outlined in ICD 301:

> Open-source intelligence is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (ICD 301, 2006)

In other words, OSINT is produced from collected and processed information from the public domain (OSINF). Examples of OSINT can be described as "…publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings", collected and processed into OSINT according to the DNI Web site, http://www.dni.gov. The DNI further explains how OSINT is viewed by the IC, in that OSINT is a collection discipline whose "…open-source collection responsibilities are broadly distributed through the IC, the major collectors are the DNI's Open Source Center (OSC) and the National Air and Space Intelligence Center (NASIC) (DNI Web Site, 2014). For a complete list of acronyms utilized throughout this paper, please refer to Appendix A, List of Abbreviations.

OSINT – An Important Part of the IC

Although the primary focus of this thesis is on OSINT, it is only one source of intelligence within the U.S. IC. For this discussion and as we will discuss in detail in Chapter 2, OSINT has always been an important part of U.S. intelligence throughout the history of the IC. All of the types of primary intelligence collection disciplines, save for Human Intelligence (HUMINT), are based on the IC use of advanced technologies to collect and process information into intelligence. Table 2 below details the primary IC collection disciplines and includes a brief description of their origins.

Table 2

Most Common Intelligence Disciplines

Intelligence Discipline	Description
MASINT	Measurement and Signatures Intelligence (MASINT) is intelligence produced through quantitative and qualitative analysis of the physical attributes of targets and events to characterize and identify those targets and events.
HUMINT	Human Intelligence (HUMINT) is the collection of information—either orally or via documentation— that is provided directly by a human source.
GEOINT	Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery, imagery intelligence (IMINT) and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth.
SIGINT	Signals Intelligence (SIGINT) is intelligence gathered from data transmissions, including Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT). SIGINT includes both raw data and the analysis of that data to produce intelligence.
OSINT	Open-Source Intelligence (OSINT) is intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.
Adapted From: U.S. National Intelligence, An Overview 2013, ODNI	

The Intelligence Cycle – Common Framework

The 9/11 Commission Report (Kean & Hamilton, 2004) and the IRPTA (2004) both recommended that OSINT be worthy of and receive discrete attention. Both reform efforts noted that OSINT needed to be used more by the IC. In the National Defense Authorization Act (NDAA) of Fiscal Year 2006, language stated that OSINT is a valuable contributor to national intelligence and should be included in intelligence analysis. The NDAA of Fiscal Year 2006 stated that "The production of open-source intelligence is a valuable intelligence discipline that must be integrated in the intelligence cycle to ensure that United States policymakers are fully and completely informed" (2006, Sec. 931, para.a.3). An important part of answering the key question of this thesis, why technologies haven't fixed OSINT, requires an understanding of how technologies have been implemented in the past to improve how OSINT is conducted, as well as how technologies may positively impact the processes and procedures within the steps of the intelligence cycle.

The intelligence cycle is the IC analytical process used to answer intelligence questions, classified or unclassified. The main steps of the intelligence cycle are Planning and Direction, Collection, Processing and Exploitation, Analysis, and Dissemination. These steps of the intelligence cycle are the generally accepted methodology used in the production of intelligence within the IC, and has been compared to the scientific method used by academic researchers when setting out to test hypotheses. When describing the goal of the intelligence analyst and the outcomes of intelligence analysis, Christopher Brown-Syed (2011), editor of Library & Archival Security, related that "Though the actual steps involved in the intelligence cycle resemble those of all scholarly research, intelligence analysis is an inherently riskier venture than scholars normally undertake…" (Brown-Syed, 2011, p. 6). For a graphical representation of the U.S. Intelligence Cycle, see Figure 1 below, retrieved from the IC Web site www.intelligence.gov (2013).

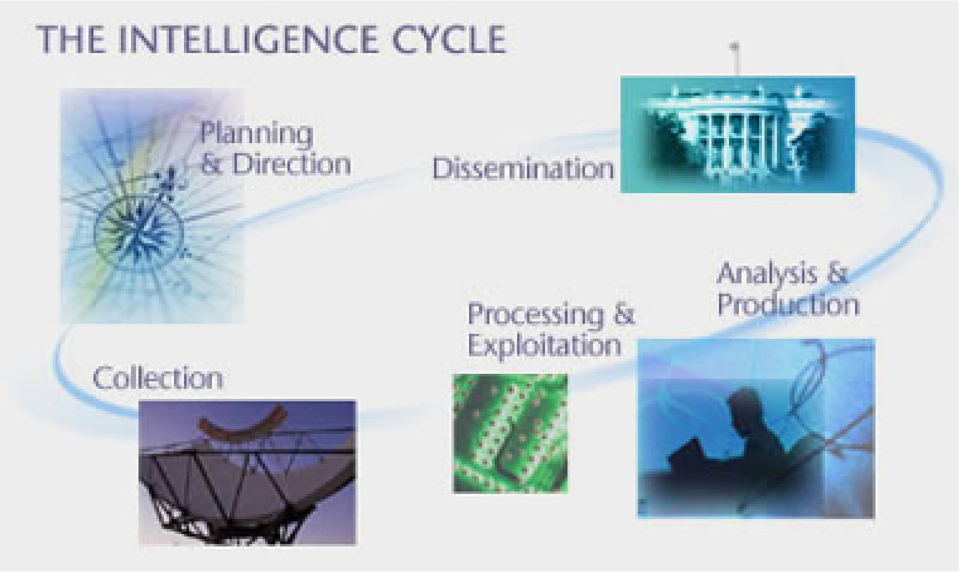


Figure 1. The Five Steps of the Intelligence Cycle

Common practices. To review past technological efforts aimed at improving how OSINT is conducted within the IC, we can look to an example from private industry. In this case, how certain information tools and technologies impact the processes and procedures found within the steps of the intelligence cycle. A commonly used method to review how well competitive intelligence (CI) technologies and software packages is to compare them to the competitive intelligence cycle, which closely resembles the IC's intelligence cycle. Fuld & Company, a leading IT company involved in private sector CI efforts, produced a report in 2007 (and again in 2013) that reviewed then-current competitive intelligence tools for prospective businesses to consider when planning for, or choosing tools and technologies to assist in their CI activities. FULD rated the software based on established criteria, centered on how many steps of the CI intelligence cycle are met by the technologies functionality (Fuld & Company, Risk & Reward Technology, 2007).

Numerous commercial vendors who exhibited at the 2007 DNI sponsored Open Source Conference, as well as at other technology expositions attended by the author, focused their marketing materials, personal discussions, and tailored presentations in a similar method as Fuld & Company, by highlighting how well their tools and technologies addressed key steps of the IC's intelligence cycle. Following this methodology, and as an aid in organizing the findings of this examination, the intelligence cycle serves as a framework for organizing past IC attempts at the implementation of tools and technologies for OSINT in a way that is easy to understand.

The discussion of IC adopted technologies for OSINT in Chapter 3 will not focus on a particular rating of a tool or technology or even how well they improve various intelligence processes or procedures found necessary to automate steps of the steps of the intelligence cycle. The intelligence cycle will be used to organize and group past IC attempts to harness information tools and technologies to improve OSINT practices. During the discussion in Chapter 3, the five major steps of the intelligence cycle will be further defined outlining the desired benefits that tools and technologies should address when adopting IT solutions within the IC. First, we examine the IC and its origins, structure, and leadership.

The IC Defined

The first definition of the IC was enacted into law in 1992 (Intelligence Authorization Act for Fiscal Year 1993, 1993), although the IC was established in 1947. The intelligence community consists of agencies and departments who work both separately and together to fulfill the nation's foreign relations and protection of the United States of America. The IC is a diverse community, and represents 17 government agencies or portions of agencies dedicated to intelligence production, including the DNI who is charged with overseeing the entire effort. Each IC agency has its core responsibilities and areas of expertise shaped to answer its specific customer intelligence requirements, as well as to contribute to the overall mission of the IC. IC members often collaborate with other members to satisfy intelligence requirements and objectives, even more so in the last 10 years in response to intelligence reforms and commission recommendations. Members also collaborate outside of government with industry and academia, as necessary, to meet mission requirements. Figure 2 provides an overview of the members of the U.S. IC as retrieved from the IC Web site www.intelligence.gov (2012).

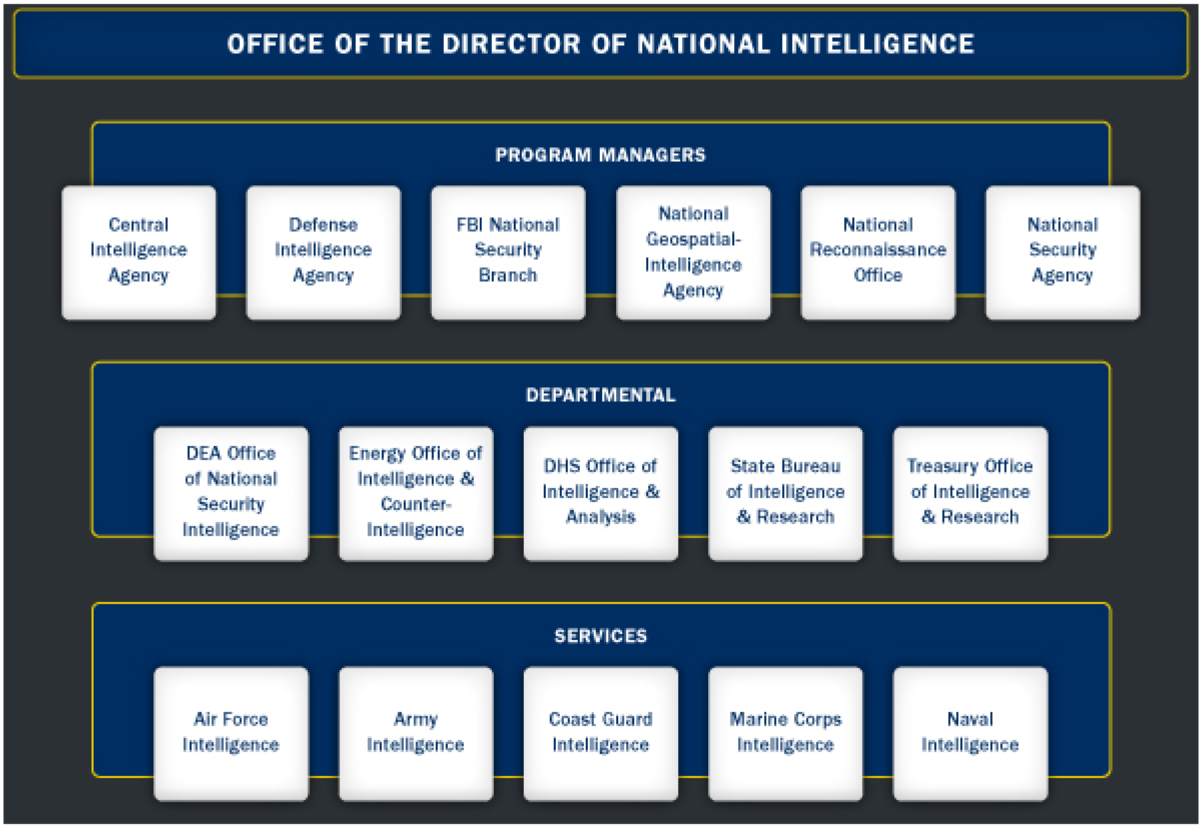

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PROGRAM MANAGERS
Central Intelligence Agency
Defense Intelligence Agency
FBI National Security Branch
National Geospatial-Intelligence Agency
National Reconnaissance Office
National Security Agency
DEPARTMENTAL
DEA Office of National Security Intelligence
Energy Office of Intelligence & Counter-Intelligence
DHS Office of Intelligence & Analysis
State Bureau of Intelligence & Research
Treasury Office of Intelligence & Research
SERVICES
Air Force Intelligence
Army Intelligence
Coast Guard Intelligence
Marine Corps Intelligence
Naval Intelligence

Figure 2. U.S. IC Members

IC agencies and missions. The IC is comprised of 17 agencies or portions thereof, and performs a myriad of missions in support of the U.S. Government. Table 3 below summarizes IC members, roles, and their primary mission as adapted from the IC Web site www.intelligence.gov in 2014.

Table 3

Intelligence Community Members, Roles, and Missions

Intelligence Community Member (Alphabetical Order)	Role	Primary Mission
Director of National Intelligence	Leadership	IC Governance
Air Force Intelligence	Service-level	Supports conduct of military operations; production of intelligence within IC
Army Intelligence	Service-level	Supports conduct of military operations; production of intelligence within IC
Central Intelligence Agency	National Center	Produce foreign intelligence on national security topics; conduct counterintelligence and other special activities related to foreign intelligence
Coast Guard Intelligence	Service-level	Maritime homeland security mission
Defense Intelligence Agency	National Department of Defense Center	Major producer and manager of Intelligence for Department of Defense
Department of Energy*	Intelligence Entity	Provide information on foreign nuclear weapons, nuclear weapons, and energy issues
Department of Homeland Security*	Intelligence Entity	Security and protection of nation's domestic assets
Department of State*	Intelligence Entity	Produce intelligence to support foreign policy and national security
Department of the Treasury*	Intelligence Entity	Economic, political, and security issues of the U.S.
Drug Enforcement Administration*	Intelligence Entity	Produce illegal drug trafficking information for the IC
Federal Bureau of Investigation*	Intelligence Entity	Intelligence support to national security, homeland defense, and law enforcement entities
Marine Corps Intelligence	Service-level	Supports conduct of military operations; production of intelligence within IC
National Geospatial-Intelligence Agency	National Center	Provide geo-spatial intelligence support to IC and combatant commands (military)
National Reconnaissance Office	National Center	Space related technology support for the IC
National Security Agency	National Center	Produce foreign intelligence related information; nations cryptography support
Navy Intelligence	Service-level	Supports conduct of military operations; production of intelligence within IC
* indicates only portion of the agency is a member of the Intelligence Community		

Adapted From: www.intelligence.gov, 13 March 2014

For a detailed description of the various components of the IC, see the publication U.S. National Intelligence Community, An Overview on the DNI Web site (2013) or the IC's Web site at www.intelligence.gov.

While each member of the IC has its primary intelligence mission to answer its customers' primary intelligence requirements, similarities exist in the way that intelligence and open source information is collected, processed and exploited, analyzed, and disseminated through the use of technologies. As a whole, the IC is responsible for the collection, production, and dissemination of information to protect the U.S. and serve a wide variety of customers (The National Security Act [NSA], 1947).

IC governance. The DNI governs the overall mission requirements and direction of the 16 member agencies of the IC. The DNI represents the IC to the President of the United States (POTUS), to the U.S. Congress, and other senior government officials. The DNI has established statutory authority over IC fiscal issues, sets forth ICD's, and assists in the planning and funding allocations for intelligence efforts conducted by the DoD, which comprise a large portion of IC member and intelligence efforts.

Why OSINT?

There are three major factors to why the IC is interested in utilizing more OSINT in finished intelligence production. Changing global threats over the last several decades require that the IC answer questions on a larger variety of global threats, from both traditional military threats to more asymmetrical threats. The second factor stems from the growing amounts of global information now available within the public domain. The last factor lies in the growing amounts of information technology that have been ingrained in our daily lives. We now briefly examine each in the following sections.

Changing global threats. The nature of the changing global threats for the IC generated calls for the inclusion of more OSINT in intelligence analysis. For decades, the IC built its intelligence agencies, workforce, processes, technologies, and capabilities focused largely on its Cold War nemesis - the former Soviet Union (Nance, 1994). The IC mission has changed immensely since the end of the Cold War. In the 1990's, emerging threats appeared across the global landscape, seemingly from every corner. The IC had no choice but to begin to adapt its workforce, technologies, and position its capabilities to readily examine potential threats across a wide spectrum of new actors.

No longer focused on a single foe, the IC had to shift focus on a larger set of intelligence requirements, mainly how to closely monitor and track threats in 80 plus countries that threaten Western interests, utilizing intelligence procedures, technologies, techniques, and methods developed during the cold war (Nance, 1994). In order to accomplish this global mission, the IC would have to rely not only on its clandestine intelligence techniques, but on the wide amount and variety of publicly available information that could be used as OSINT. Col. Mick Nance, then a student at the U.S. National Defense University, wrote that the mission of the IC had almost become "mission impossible" due to the changing threat environment (Nance, 1994, p. 3).

Perhaps the most vocal and most recognized OSINT advocate over the last 20 years has been Robert Steele, a former CIA analyst, former senior leader of the Marine Corps Intelligence Activity. Predating official IC public forums on OSINT by over a decade, Steele organized the First International Symposium on Open Source Solutions in 1992, with senior IC officials participating (Studeman, 1993). Admiral William Studeman, then Deputy Director for Central Intelligence (DDCI), related during remarks how the IC was changing as a result of their new found missions in the post cold-war environment. “In the new global environment, open sources provide much more hard, credible data about a wide range of international political, social, and economic issues” (Studeman, 1993).

Lieutenant General James R. Clapper (1994), then Director of the Defense Intelligence Agency (DIA) and now the current DNI, wrote of the changing intelligence mission in 1994’s “Challenging Joint Military Intelligence”. Clapper echoed sentiments related to the complexities the IC faced after the demise of the Soviet Union and communism, the dissolution of the Warsaw Pact, and increased United States involvement in United Nations peace keeping operations in IRAQ, Somalia, and the Balkans as having an impact on the way in which the U.S. conducted its intelligence mission. In 1994, Clapper stated that “Today’s threats are different from yesterdays and in many respects considerably less predictable” (Clapper, 1994, p. 94).

Dr. William Lanheman (2010), a retired naval surface warfare officer and Associate Professor of Homeland Security at the Embry-Riddle University, and a Senior Research Scholar at the Center for International and Security Studies at Maryland of the University of Maryland’s School of Public Policy, noted that the IC will continue to face challenges created by globalization as future security threats will be of a “…much smaller scale…” and their cumulative effects “…might produce extremely destabilizing and destructive results…” (Lanheman, 2010, p. 203).

The IC continues to address the immense challenges it faces within the global threat environment over two decades later. After nearly a decade of combat operations in Afghanistan and Iraq, these operations are concluding, and the POTUS outlined in 2012 that the new U.S. national security strategy which included even broader national security challenges for the U.S., including the “security and prosperity of the Asia Pacific”. A 2012 task force report noted that future efforts would draw heavily on the nation’s intelligence, diplomatic, and military forces (Intelligence and National Security Alliance [INSA], Expectations of Intelligence in the Information Age, 2012, p. 2).

The Intelligence and National Security Alliance (INSA), a non-profit, non-partisan, public-private organization that works to promote and recognize the highest standards within the national security and intelligence communities, published a white paper in 2012 titled “Expectations of Intelligence in the Information Age”. This paper originated from the INSA Rebalance Task Force and defined some of the broad issues that U.S. Intelligence would be required to provide early warning to U.S. policy makers. INSA argued that these non-traditional security threats and other issues need to be covered by today’s IC to answer a broad set of standing requirements from U.S. policy makers. These requirements cover:

- The advent of political movements, fueled by modern telecommunications and social media, in opposition to weak, corrupt, or authoritarian government
- The destabilizing effects of emigration, immigration, and massive demographic shifts
- The corrupting influence of interlocking or overlapping networks engaged in illicit activities related to financial fraud and money laundering
- The smuggling or marketing of weapons, drugs, commodities, and people

- The exploitation of vulnerabilities within the global communications network to undermine the security of governments, private sector entities, and individuals who are increasingly dependent on that network
- Localized but widespread shortages of food, water, and preventative medicines
- The effects of disruptive secular, ethnic, and sectarian strife
- Unrest leading to conflicts fueled by political repression, economic depression, or the failure of governments to meet the essential needs of the population (INSA, Expectations, 2012, p. 5)

INSA also noted that these new intelligence requirements are in addition to the traditional threat analysis, military, and security requirements that the IC has conducted and will continue to conduct moving forward.

The globalization of information. While the IC was refocusing, and reorienting its efforts against the new global threat environment, the globalization of information found previously closed societies opening their doors to the information revolution made possible by the Internet. These newly available sources of information would be viewed by those in the IC as a blessing, and potentially as a curse. These new found sources of information would help address emerging IC desires to answer a new era of intelligence questions, covering worldwide topics and issues not possible through the established cold-war focused collection posture. These new found sources of information would often provide the only information on a given set of topics, or about events or occurrences within a particular country.

John C. Gannon (2000), then National Intelligence Council (NIC) Chairman, spoke on the changing nature of threats that the IC faced in 2000, along with the increasing amount of publicly available information that could be used for intelligence analysis:

> First, open-source information today is more important than ever in the post-Cold War world, in which intelligence targets are more diverse in complexity and more dispersed in geography. Closed societies in the Former Soviet Union and in Eastern Europe have opened up, and reliable information now proliferates. The revolution in information technology, at the same time, has vastly increased the volume and speed of the information flow across the globe and across our computer screens. Open-source information now dominates the universe of the intelligence analyst, and this is unlikely to change for the foreseeable future. (Gannon, 2000)

In 2001, the Central Intelligence Agency (CIA) Global Futures Partnership in the Directorate of Intelligence published “Are You Ready? Implications of a Changing Global Information Environment for Open Source Intelligence” (GFP, 2001) and presented overall conclusions of “...Open Source 2010, a CIA-led unclassified effort to consider the implications of such developments as globalization…and the rise of the Internet on collecting and analyzing publicly available information” (p. i). Its findings projected that OSINT played a significant role in the future of the IC due to the changing information environment across the world.

Richard A. Best, Jr. wrote in “Intelligence Issues for Congress” in 2006 about the importance of OSINT given the requirements that now exist for information about many regions and topics. The globalization of information would require that the IC cover more topics and issues from a variety of countries, instead of the former concentration on military and political issues of a few. It is interesting to note that in 2006, Best referred to OSINT as an "another category of information", and was not listed amongst the other intelligence disciplines found in the IC (Best, 2006, p. 5).

Since 9/11/2001, the IC has been focused on these global threat issues, as well as focused on a different kind of enemy. The previous IC focus on nation-state actors began to shift to focusing on a more unconventional, or asymmetrical threat. Global conflicts and the growth of world-wide terrorism capabilities meant that the IC had to develop capabilities it previously did not possess. The IC has spent the last ten years plus building an intelligence apparatus that would have to be able to focus on traditional threats, unconventional threats, and on homeland security.

Growth of information technology. The influence of technology over the last twenty years on our daily lives is immense. Cellular technologies brought mobile communication capabilities. Computers designed and built for home use litter the marketplace. The rise of the Internet has provided access to more global information than imaginable in the 1980s. Fiber-optic technologies, in some cases, replaced out-dated satellite communications with an ever faster and more efficient way in which to send and process information across long-distances. Automobiles have more technologies than ever before, much to the chagrin of last generation mechanics. Individuals now carry portable information and communication devices in their pockets that have more advanced technologies than used in the first space shuttle. These devices continue to shape the ways in which we communicate with each other and the world around us.

Information technologies have been developed over the last 30 years that have made profound impacts on the ability to communicate, discover and share information, conduct commerce, and keep informed on issues due to the 24 hour news cycle. The growing diffusion of advanced information technologies stemming from the private sector have given rise to industry information giants like Google, Amazon, Facebook and Twitter to name a few. The continuing rise of advanced information technologies on a global scale have provided the opportunities for world-actors to develop new technologies previously only realized by the U.S.

The IC built capabilities and technologies throughout the Cold War aimed to maintain a technological superiority against the Soviet Union. However, now the world was changing, and the Internet as a technology provided potential adversaries, both individual actors and nation states, to develop information and technological capabilities that far surpassed those of the previous enemy. These developments began to worry senior IC officials over the technological advantage maintained by the U.S., specifically within the IC, compared to over 20 years ago. In 1992, Studeman discussed then established requirements to update the IC's approach to handling the vast amount of open source information available within the public domain. In regards to OSINT, Studeman reported that a Community-wide Open Source Steering Council had developed a Strategic Plan with a vision of the IC goals over the next 10 years (to the year 2002). One of the components of this forward looking plan was the suggestion that the IC will have to get creative to deal with harvesting new sources of potential intelligence data. He offered "As we look to the future, we will have to develop more creative approaches to manage the vast amount of data being produced" (Studeman, 1993).

John Perry Barlow (2002), the cofounder of the Electronic Frontier Foundation, captured future Principal Deputy DNI Gen. Michael V. Hayden, USAF (ret.) sentiments regarding the importance of getting over the Cold War, and exploring new technologies to help solve intelligence issues. Hayden noted that the U.S. must shift its thinking in regards to the technological stature of our future adversaries, versus our former primary foes, and noted that:

> Our targets are no longer controlled by the technological limitations of the Soviet Union, a slow, primitive, underfunded foe. Now [our enemies] have access to state-of-the-art....In 40 years the world went from 5,000 stand-alone computers, many of which we owned, to 420 million computers, many of which are better than ours. (Barlow, 2002).

The USA remains the technology leader in the world today, and has long embraced the benefits of technologies to improve society. Likewise, the IC has consistently sought the latest and greatest technologies to provide intelligence solutions to best answer national security questions. In order to meet the security requirements of the 21st century, the IC realized that it must build improved capabilities, be creative and adaptive in regard to information technologies in order to accomplish their assigned missions. The U.S. IC is one of the world’s biggest information based “businesses”, and relies on a myriad of IT and communications solutions to conduct its business of intelligence. The IC will necessarily be required to continually develop, and nurture information technologies in the coming years to solve many issues within intelligence. The growing reliance on and use of OSINT in finished intelligence production requires that the IC fully build new and innovative information technologies to continue to maintain the technological edge over our potential adversaries in the future.

Thesis Limitations

To explore this topic, the author conducted a review of technologies employed within the IC that had particular applications regarding OSINT. This review focused on both government and private sector produced reports, documents, speeches, and literature on a variety of subjects related to the U.S. IC. The information technologies reviewed in Chapter 3 were selected based on information obtained during research, or from a variety of other publically available sources of information. It is possible that more advanced or different technologies may be implemented within the IC aimed at improving OSINT. However, publicly available information about these technologies may not exist due to the closed nature of the U.S. IC, and the practice of protecting sources and methods. Classified technologies, those not exposed or discussed legally outside of the IC, can not be examined in this thesis. However, the literature is quite rich on OSINT's rise and relative popularity over the last 20 years. The amount of literature surrounding OSINT and its importance, opportunities for greater use, ideas for restructuring OSINT efforts within the IC, etc., presented the author with an immense amount of information to consider. A substantial body of evidence on this topic, when examined in toto, adequately provides the context and the framework for this examination and addresses the original thesis questions and conclusions. The author aimed to provide salient examples addressing key issues that would adequately represent key trends, observations, and limitations. Any omission of information lies on the author. Like the thesis topic, OSINT, this examination relies solely on publicly available information.

Thesis Summary

The goal of this thesis is to show why technological solutions aimed to improve the ways in which OSINT is produced and utilized within the IC have proven to be difficult. This thesis aims to outline why technological solutions alone aimed to solve the myriad of OSINT issues may not provide the outcome OSINT insiders and advocates may desire.

Chapter Summaries

Chapter 2 provides a review of how OSINT becomes important again to the U.S. IC. It discusses the information explosion, and some recommended solutions for the IC in regards to OSINT, and establishes that the use of information technologies is often at least part of the recommendation for improving how OSINT is produced and utilized by IC intelligence analysts.

Chapter 3 highlights past IC attempts to implement a myriad of information technologies aimed at improving how OSINT is conducted within the IC. This discussion is framed by the intelligence cycle, the method from which intelligence is produced, and will discuss how these technologies are aimed to improve the processes therein. Particular emphasis is placed on the types of technologies that can automate processes in the production of OSINT to free up more time to be spent on analysis.

Chapter 4 reviews key aspects of the IC as a socio-technical system, and its practices, processes, culture, leadership, and other factors may be limiting the progress of OSINT within the IC thus far.

Chapter 5 concludes with an examination of what happened to OSINT in the years since the 2006 NOSE OSINT Vision was published and where OSINT is headed.

The chapter continues with an examination of some long-term issues that will continue to challenge the conduct of OSINT within the IC. We then discuss some OSINT successes that have been achieved along with a discussion on developing trends to watch. Chapter 5 concludes with an examination of the likelihood of substantive changes for OSINT and provides conclusions on why haven't technologies fixed OSINT thus far.

CHAPTER 2

HOW OSINT BECAME IMPORTANT (AGAIN)

> "The world abounds in open information to an extent unimaginable to intelligence officers of the Cold War." (Stephen Mercado, 2004)

As outlined in The National Security Act of 1947, and since the inception of the IC, OSINT has been noted as being an important source of intelligence (NSA, 1947). Dr. Donald Madill (2005), a former military intelligence officer, related in an essay that during the 1947 Senate hearings, intelligence experts "…testified that a proper analysis of information gained through open sources could satisfy at least 80 percent of our peacetime intelligence requirements."(Maddill, 2005, p. 19). Madill also related that the problems of today's information overload are not new, and that the "virtually staggering" volume of the material obtained could possibly present obstacles to exploiting it (Madill, 2005, p. 22).

Nearly a half-century later, Studeman (1993) provided a key note presentation at the First International Symposium on Open Source Solutions in 1992, organized by Robert Steele. Studeman accounted for many of the long-running arguments in support of OSINT. He listed many positive uses of the OSINT over the years, including the successes of the Foreign Broadcast Information Service (FBIS) since its inception. He also noted many examples over the years when OSINT was often the only intelligence the IC had regarding world events, including the 1956 Hungarian uprising, and the 1968 invasion of Czechoslovakia. Studeman spoke about the positive benefits of OSINT - its value in producing early warning, or indications and warning (I&W) of certain events, and the importance in the combination of OSINT with other traditional classified information when performing intelligence analysis. Another keynote speaker at this symposium, George Keyworth, the former science adviser to the White House, noted that "…the absorption of open source materials into the intelligence process takes place against a background of widely distributed information processing technologies and foreign policy issues" (Symposium Speakers Define Strategic Plan For Using Open Source Intelligence, 1992, para. 5).

Shortly after the fall of the Soviet Union, and in the early days of the information explosion, the IC recognized the need for sharing of OSINT within its members, beyond traditional intelligence dissemination methods. In response, the Director of Central Intelligence (DCI) established the Community Open Source Program Office (COSPO) in the Central Intelligence Agency, through the Director of Central Intelligence Directive 2/12 in 1994 (DCID, 1994). The objectives of COSPO were to oversee all aspects of OSINT, to include administrative coordination, advocacy, and the identification of requirements, and to ensure funding for open source activities within the IC. COSPO was also charged to coordinate IC systems architecture, assess employed technologies and procedures, as well as evaluate promising alternatives to be used for OSINT. A major function of the COSPO was to "coordinate the development of new processing and exploitation tools and promote the integration of automated data processing tools developed elsewhere" (DCID 2/12, 1994). The formation of COSPO highlighted the IC's desire to develop or acquire new information technologies to be used for OSINT some twenty years ago.

Over the last several decades, various government and intelligence reform commissions have espoused the importance of using OSINT while performing intelligence missions relating to the safety and security of the United States. The Commission on the Roles and Capabilities of the United States Intelligence Community, hereafter the Aspin-Brown Commission, was created in 1994 and was charged with examining U.S. Intelligence activities in the "post-cold war global environment" and with preparing a report of its findings and recommendations to the President and the Congress (Brown, 1996, p. 3). Its findings, published in 1996, made it clear that accessing the available information in the public marketplace (potential OSINT) was necessary to ensure that intelligence analysis included relevant information from all sources. The commission also recognized that accessing this information was also becoming more difficult; while the number of databases of open sources was increasing, analysts had limited access to them. The report asserted that open sources "…do provide a substantial share of the information used in intelligence analysis" (Brown, 1996, pp.88-89). The report also criticized the U.S. IC for failing to make greater use of open source intelligence. Perhaps the most significant finding from this commission relevant to this discussion, found that:

> An adequate computer infrastructure to tie intelligence analysts into open source information does not appear to exist. In the view of the Commission, the creation

> of such an infrastructure should be a top priority of the DCI and a top priority for funding. (ABCR, p.89)

In 1996, a non-official Independent Task Force of the Council on Foreign Relations provided similar views in a report entitled *Making Intelligence Smarter: The Future of U.S. Intelligence*. This non-official entity recommended that “The intelligence community should make maximum use of open sources…” (Greenberg & Haass, 1996, p. 4).

OSINT Gains Momentum

OSINT’s importance grew as the U.S. fell victim to the deadly attacks from a new adversary, actors of a non-nation state, an adversary with no national sponsor, Al Qaeda. Post 9/11 discussions focused on how the IC failed to warn of this threat and outlined many necessary intelligence reforms. One of the major recommendations included the need to utilize more OSINT within the IC and advocated for the creation of a new open source intelligence agency to ensure the widespread use and availability of open source intelligence for the IC. In section 1052 of the IRPTA 2004 (2004), this newly crafted law doubled down on the 9/11 commission findings and put forth recommendations that directed the newly created DNI to create a national open source agency, to ensure that members of the IC used OSINT consistent with each agencies mission, and argued that OSINT was important and must be integrated into the intelligence cycle to ensure that U.S. policy makers are “fully and completely informed” (IRPTA, 2004, section 1052).

IC Consensus

Following the creation of the Office of the DNI (ODNI) along with the establishment of the OSC, the DNI issued ICD 301 which prescribed OSINT activities within the IC. One of the many recommendations for OSINT revolved around ensuring that OSINT was championed by central IC leadership. As has been previously discussed, the DNI quickly established the ADDNI/OS as the IC's chief OSINT advocate. The ADDNI/OS, Mr. Jardines, formally implemented the NOSE OSINT vision in 2006. The issuance of this vision was among the first steps in the attempt to raise OSINT's stature within the IC. OSINT was clearly being established as a priority issue within the IC and appeared to be on an upward trajectory in 2006.

OSINT may have reached its peak of popularity within the IC noted by the DNI sponsored Open Source Conference held in the summer of 2007 in Washington, D.C. This conference was the first government sponsored, public event aimed at showcasing the importance of OSINT to the IC. This conference also provided a forum for private sector technology firms to showcase their products and services designed to help the IC to tackle emerging OSINT issues. The author conducted personal discussions with some of the private sector exhibitors at this conference which resulted in key insights about the business and technological side of OSINT. These discussions also led to the initial research that led to this thesis. Keynote presentations at the conference featured senior leadership of the IC and included the DNI, the ADDNI/OS, Mr. Jardines, among others. Clearly, the importance of OSINT to the U.S. IC was put on the world stage for all to see.

Richard Best and Alfred Cummings (2008), both specialists in the Foreign Affairs, Defense, and Trade Division, Congressional Research Service (CRS), summarized OSINT's importance for Congress in 2007 and again in 2008 in "Open Source Intelligence (OSINT): Issues for Congress". Regarding OSINT's place within the IC, the authors reported that:

> A consensus now exists that OSINT must be systematically collected and should constitute an essential component of analytical products. This has been recognized by various commissions and in statutes. Responding to legislative direction, the Intelligence Community has established the position of Assistant Director of National Intelligence for Open Source and created the National Open Source Center. The goal is to perform specialized OSINT acquisition and analysis functions and create a center of excellence that will support and encourage all intelligence agencies. (2008, para. 2).

The long running importance of OSINT to the IC can not be understated, and its importance to the IC is clear throughout it's nearly seven decades. The roles of information and communication technologies within the OSINT discussion are central to understanding how the IC has conducted business since the IC's inception.

The Information Explosion

The information explosion over the last several decades has largely been caused by the diffusion of the Internet and the World Wide Web (WWW). The information explosion has created serious challenges for the IC in trying to keep up and use of all of the new types of information that were previously unavailable. The landscape of information technologies were also beginning to change. Over twenty years ago, it became apparent that the world was changing and that an abundance of publicly available information was being created daily. IC OSINT efforts were concentrated in the FBIS, the main collector of foreign media sources and producer of OSINT for the IC, increased in scope and scale. A 1993 article "What Is Open Source Information?" (1993) captured Studeman's insights into the breadth and depth of OSINT efforts being performed by the

FBIS. Studeman recounted technological successes and necessary improvements in ongoing IC OSINT efforts, noting that:

> For decades the CIA has been collecting, analyzing, and reporting on foreign news sources through the Foreign Broadcast Information Service (FBIS). Each day FBIS monitors nearly 800 hours of TV from 50 countries in 29 languages; it routinely reviews 3,500 publications in 55 languages, roughly one million words daily. The magnitude of this effort has placed a premium on timely translation services, storage, and filtering the voluminous data looking for key events ("What Is Open Source Information?" 1993, para. 3, 1993).

The explosion of the Internet during the 1990's gave rise to an even more abundant source of world-wide information. Lawrence Wright, an author for The New Yorker, wrote a 2008 article on then DNI Mike McConnell. Wright noted that McConnell previously served as the Director of the National Security Agency (DIRNSA). McConnell recalled that in 1992 when he assumed the position of DIRNSA, the Internet and e-mail were radically expanding the abilities of terrorists and rogue states to communicate. "When I went there in '92, the Internet existed—it was called Arpanet—but the World Wide Web did not," McConnell recalled. "Then the Web made the Internet accessible for everybody. My world exploded" (Wright, 2008).

With the rise of the Internet's popularity, its use as an information source to IC analysts increased. The growth of search engine technologies on web browsers made it easy to type in a question and wait for the search results to be returned. In the 1990's, however, finding relevant or pertinent information on the WWW was a challenge. Traditional search methods and their results would easily overwhelm users (and analysts) with information. Results obtained through traditional search engines often only served to complicate the analyst's job by providing too much information to search through. Too much information on the WWW led to difficulty in finding pertinent and useful information to be produced as OSINT. Richard S. Friedman (1998), a retired U.S. Army Colonel, former CIA senior analyst, and assistant national intelligence officer, noted the difficulties in receiving too much information when conducting intelligence analysis:

> Intelligence consumers, government officials, and policymakers have not been complaining about a shortage of information; they are suffering from a saturation. The flood of mass-produced data now available and the ensuing overload means that collection is no longer the principal problem. The greater challenge facing intelligence organizations is analysis, consolidation, and timely dispatch of data and results to the individuals who need it. (Friedman, 1998, pp.159-165).

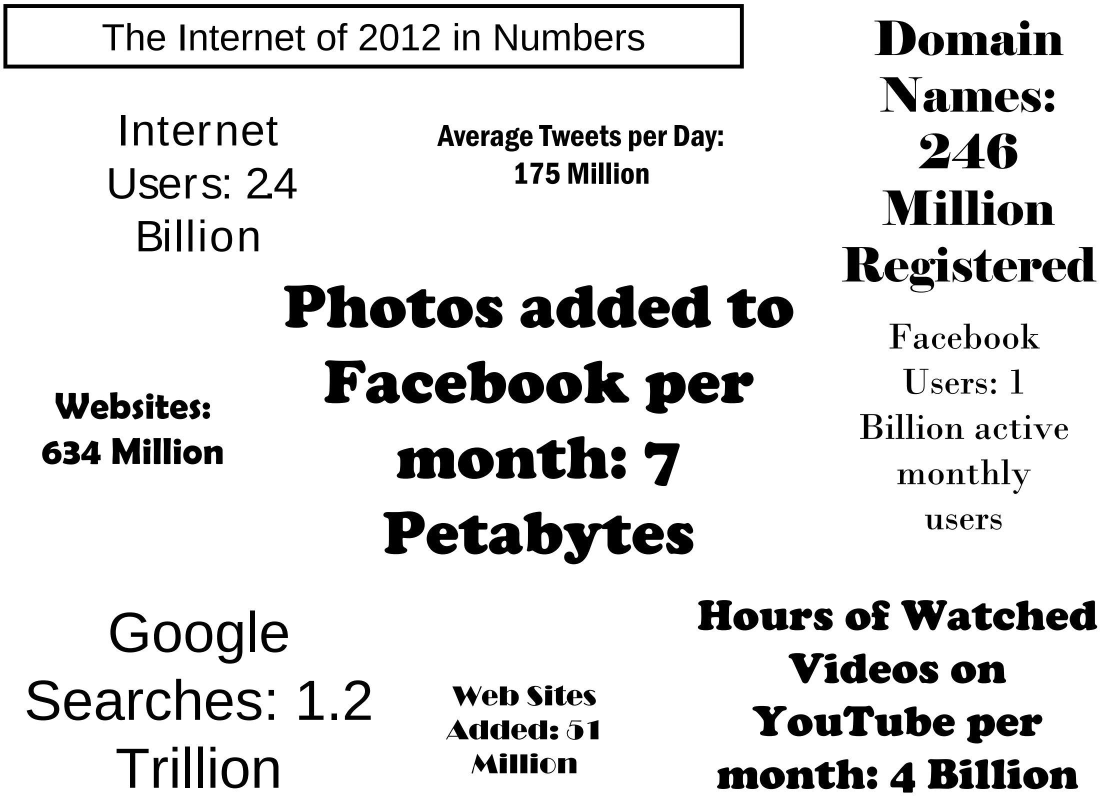
Echoing Friedman's sentiments, Gannon (2000) related that open source was not just coming from media reports, but from a "…vast array of documents and reports, which are publicly retrievable but, nonetheless, often hard to retrieve from today's high-volume, high-speed information flow" (Gannon, p. 153). Margaret MacDonald, a Senior Editor at the MITRE Corporation in Bedford, Mass., and Anthony Oettinger, a Gordon McKay Professor of Applied Mathematics and Professor of Information Resources Policy at Harvard University, co-authored an article in the Harvard Review (2002) which outlined the growth of information technologies within the IC and pointed to the growing issue of information overload. Their report cited that unlike Cold War periods where there was sometimes a dearth of information due to the closed nature of our adversaries, the IC no longer suffers from "…information scarcity but from information overload" (MacDonald

& Oettinger, 2002, p.44). Formerly impenetrable countries began to adopt new global information technologies to take advantage of the emerging flow of world-wide information. Madill (2005) added his insights in 2005 into the emerging global information explosion:

> Formerly closed societies have begun to allow us access to information that was previously state secrets. The "Information Superhighway," with all its international connections, has given us access to much more information; there are few roadblocks or restricted-access routes for those who know what to look for and where to look for it. Under these conditions, the percentage of requirements that can be satisfied from open sources should be at least as great in the twenty-first century as it was in 1947. (Madill, 2005, p. 19)

Arnaud de Borchgrave (2007), editor at large of The Washington Times and of United Press International, related in a Washington Times commentary the changing nature of OSINT and the deluge of information sources available and how this change has made the intelligence business "…infinitely more complex" (de Borchgrave, 2007, p. B04). He added that the growing amounts of information available in the marketplace on Web sites, blogs, YouTube, flickr.com, along with the growing amount of personal electronic devices continue to provide additional sources of potential OSINT that would have to be monitored. Borchgrave claimed that the input to the Internet doubles every six months, and that the growth of available data that moves across the globe daily equates to "…several thousand times the entire contents of the Library of Congress…" (de Borchgrave, 2007, p. B04).

The state of information explosion in 2007 has since been usurped in the years since. Figure 3 below highlights some key statistics from 2012 showing the amount of information being posted or created on the Internet, as adapted from the Web site www.royalpingdom.com (2014).



The Internet of 2012 in Numbers

Internet Users: 2.4 Billion

Average Tweets per Day: 175 Million

Domain Names: 246 Million Registered

Photos added to Facebook per month: 7 Petabytes

Websites: 634 Million

Facebook Users: 1 Billion active monthly users

Google Searches: 1.2 Trillion

Web Sites Added: 51 Million

Hours of Watched Videos on YouTube per month: 4 Billion

Adapted from Source: http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/ - accessed 1May 2014

Figure 3. The Internet of 2012 in Numbers

Proposed Solutions for OSINT

The challenges to improve OSINT within the IC are numerous. Discussing all potential or recommended solutions for OSINT are well beyond the scope of this thesis. However, many interested parties have offered suggestions or recommendations for how the IC should structure, approach, or conduct OSINT activities. Some OSINT proponents have recommended that the IC outsource OSINT efforts to private sector companies. However, the practice of outsourcing intelligence functions unable to be accomplished by government employees to government contractors is not a new recommendation, but a long established procedure within the IC.

Christopher Brown-Syed, former editor of Library & Archival Security, recommended that the IC expand roles for intelligence community librarians as IC resources when conducting OSINT activities. Brown-Syed noted that librarians, archivists, library technicians, and computing professionals involved in running today's libraries provide them with the background in information science that provide them with a "…habitual way of looking at published material…" that may prove useful in the conduct of OSINT within the IC (Brown-Syed, 2011, p. 1). This concept was also outlined in the NOSE OSINT vision published in 2006, that the IC would recognize and utilize librarians as "open source champions" (Jardines, 2006, goal 2.1).

Phil Nolan, a senior manager with IBM in Washington, D.C., suggested that the IC should adopt a curator approach to OSINT to solve issues with information overload. Nolan explained that "Curating means that IC analysts would not have to create all the analysis themselves. Instead, the analysts would need to understand and report what the wider world is saying about a topic, then show where their analysis fits into the spectrum of opinion, and why" (Nolan, 2012, p. 790). Nolan recommended a revision of the all-source analysis process that would ensure that open source analysis is anonymized and rated for reliability. The sources of the curated OSINT would come from paid U.S. sources like Stratfor, a geopolitical intelligence firm that provides strategic analysis and forecasting to individuals and organizations around the world, along with other government related think tanks, from unpaid U.S. sources like the media, weblogs, as well as from curated feeds from both formal and informal media from outside of the U.S. (Nolan, 2012, p. 793).

A provocative recommendation regarding the IC's ability to effectively produce OSINT came in 2010, with Lanheman arguing that the IC needed a new paradigm. He stressed that information comes in two basic forms that need to be managed within the IC. The first is information and knowledge that governments and actors have no interest in sharing. The second is information and knowledge that governments have reason to keep secret. He argued that single institutions (like the U.S. IC) can't manage both kinds of information. Lanheman added that the IC faced challenges when it comes to sharing "Intelligence agencies are the segment of national governments charged with making sense of future security challenges. But their traditions and organizational cultures emphasize secrecy, not knowledge sharing" (Lanheman, 2010, p. 202). Lanheman made recommendations that, if adopted, would represent a paradigm shift for the IC. He noted that the traditional intelligence required by the IC and its consumers rely on the acquisition of materials that government and actors regard as secret. He asserted that the emerging threats, transnational actors, and the vast amount of information now available in the public domain required more openness. He suggested some organizational changes for the IC and its secret entities, as well as the need to create an Office of Strategic Information (OSI) which would be responsible for OSINT production for the U.S. Government (USG) and the IC. The IC would then create a secret agency to implement advanced tools and technological innovations to fully exploit OSINT while keeping the resulting information and analysis in classified domains.

Human & Technology Solutions

To paraphrase Baxter (2011), a socio-technical system describes an environment whereby people, organizational structures, and technologies are linked together and engaged in working towards a common goal (Baxter, 2011). The IC meets this definition based on the multiple organizational structures and agencies from which it is comprised, the technologies that connect them all together, and the people who work within one of the IC agencies. The IC's common mission is to collect information needed by the President, the National Security Council, the Secretaries of Defense and State, and other government officials in the course of their assigned duties and responsibilities. Despite the numerous proposals from outside the IC for OSINT reform, IC insider recommendations for improving OSINT have centered on issues surrounding human capital (i.e., analyst training, education, expertise), or on the potential application of technologies to effectively give OSINT the edge in future intelligence analysis, or in some cases both together. A socio-technical system such as the IC will likely require a variety of innovative solutions for OSINT that affect the people, the organizations, and the technologies that bind it together in order to realize systemic change. We review some of these recommendations in this section.

Human solutions. Friedman (1998) explained the two factors that shaped the future of OSINT as "The emerging debate between investing in technology and developing competent analysts concerns itself basically with the value and role of open source intelligence" (Friedman, 1998, pp. 159-165). Gannon (2000) echoed Friedman, and related that technologies are only one part of the potential answer for the challenges of OSINT:

> …technology is a major part of the answer but it is no substitute for the other essential part, people. To deal with the open-source challenge, the Intelligence Community must invest more in technology to give us the analytical tools we need to access and exploit the vast information available to us, and in our people on whose expertise we must rely more than ever to prioritize and interpret this information (Gannon, 2000, p. 153).

The second goal outlined in the 2006 NOSE OSINT vision was the creation of "…a guild of OSINT experts who champion the use of open sources…" along with developing OSINT as a universal (IC) competency and ensuring that OSINT was embedded in all training (Jardines, 2006, Goal 2). In response to this idea, the OSC began offering training programs for individual IC analysts to train and build the requisite OSINT expertise within the IC. Susan B. Glasser (2005), a Washington Post Staff Writer, characterized comments by the former director of the OSC, Mr. Doug Naquin, in 2005 that the OSC saw itself as the repository of what Naquin termed "open-source tradecraft" (Glasser, 2005). Robert K. Ackerman (2006), editor in chief of *SIGNAL Magazine*, wrote on the DNI's OSC Open Source Academy (OSA), noting that the OSA offered nearly two dozen courses for IC analysts focusing on open source exploitation and analysis. Ackerman (2006) recounted Jardines' outlook on the importance of training analysts to develop OSINT expertise as a part of the solution. "The community in general has a very small, isolated, open-source effort". Jardines would add "There are no common standards for training or dissemination. We are looking to create, in essence, a guild of experts who can lead the way" (Ackerman, 2006, para. 5). The IC did create

OSINT training opportunities like never before in the years following the IRPTA and set out to satisfy the human half of building OSINT experts throughout the IC.

Technology solutions. Technological solutions aimed to improve OSINT have long been discussed by OSINT advocates and insiders, as noted by the earlier discussion of the long-running mission of the FBIS, now the OSC. Public discourse highlighting technological innovations and applications for intelligence continue to show the IC desire to improve the ways in which the IC capitalizes on the benefits of OSINT. At a minimum, the development, or adoption and implementation of technologies to help solve OSINT issues have been included in numerous recommendations over the last several decades.

Jami M. Carroll argued in “OSINT Analysis Using Adaptive Resonance”, that OSINT is a valuable source of intelligence that is useful in intelligence analysis. Carroll identified that a key problem is making sense of the vast amounts of information in time to prevent intelligence failures. Carroll recounts the events of 9/11/2001 may not have occurred had the IC had better IT tools, and improvements to the tools and technologies available to IC analysts are necessary to provide proper support to the defense of the nation (Carroll, 2005, p. 756).

Dr. Mark M. Lowenthal (1999), then President of Open Source Solutions (OSS USA) and a former deputy director of the CIA, noted that no technological silver bullet exists that would fix OSINT, and that technologies are only a means to the end, not the end itself. The effective implementation and use of information technologies within the IC to collect, process, sort, and provide context from vast amounts of available information is a solution that must play a central role (Lowenthal, 1999).

A majority of suggestions related to improving the ways in which OSINT is produced and utilized relies on the utilization of information technologies, thus relating to the primary research question which examines why technologies haven't "fixed" OSINT within the IC to date. Thus, this examination focuses on information technologies and their intended roles within the IC to produce, provide access, and to more efficiently use OSINT within the intelligence cycle to produce finished intelligence.

IC recognition of technology's benefits. The following sections establish that the IC knew early on in the information revolution that it must co-opt technological innovations to meet its evolving missions that required covering global threats while in the middle of the information revolution. Nance (1994) noted the importance of seizing the power of information technologies. He asserted that organizations or nations who embrace new technological advances would gain a competitive advantage. Nance also noted that the U.S. should become more adaptive in the ways in which we obtain information technologies, and until we overhaul the ways we acquire new technologies, we will never be able to catch up (Nance, 1994, p. 9).

Edward F. Dandar Jr., (1997) a retired Colonel, U.S. Army Reserve, reported key findings of both the Aspin-Brown Commission, and another publication entitled "An Intelligence Community Information Technology Assessment: Recommendations for the Future". Dandar largely agreed with the findings and provided some additional insights into the growing challenges of the information revolution on the IC. "A critical problem facing IC analysts in the Government Information Enterprise (GIE) is access to Open Source Information (OSI) and tools to help them deal with large volumes of information" (Dandar, 1997, para. 9).

Gannon also recounted the importance of investments in technologies to help manage the “information glut” (Gannon, 2000, pp. 154-5). He enumerated the need to develop analytical tools such as clustering, link analysis, time series analysis, visualization, and automated database population as efforts that were already underway in 2000. He also proposed the need to be able to access both classified and unclassified information from a single workstation, along with the requirements to standardize information and tag it so that the resulting intelligence would be easier to search, structure and put into databases.

Stephen Mercado (2004), a former employee of the CIA, also noted that technological advancements are necessary for the IC to move OSINT forward. He suggested that:

> …the Intelligence Community must organize its own technical resources and tap those of the private sector to exploit the latest information technology for OSINT collection, analysis, production, and dissemination. (Mercado, 2004)

Douglas Hart, president of Cyberneutics, Inc., an international security policy and information technology consultancy, and Steven Simon (2006), Senior Fellow for Middle East Studies at the Council on Foreign Relations, argued that information technologies can improve intelligence analysis because the IC already uses computer-based tools to produce current intelligence, and potential new recruits for the IC are the most computer literate generation in history (Hart & Simon, 2006, p. 48). Gary Ackerman, Research Director of United States Department of Homeland Security’s National Consortium for the Study of Terrorism and Responses to Terrorism, Molly James, and Casey T. Getz, both former Research Assistants of Mr. Ackerman (2007), agreed that the IC needed to improve its technologies and tools that allow the analyst to deal with the vast amount of information available to IC analysts. The authors noted that new technologies, although only one part of the solution, could be a “key component” in improving national intelligence (Ackerman, James, & Getz, 2007, p. 678). They also noted the development of new tools that allowed analysts to discover new issues and trends that they had not considered or were previously unavailable (Ackerman, et al., 2007, p. 694).

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005), hereafter referred to as the WMD Commission, in their finished report also suggested that technology can overcome many of the security concerns and deal effectively with the dense amount of data in the public domain. The WMD commission recommended that a specific office should be established to "acquire or develop when necessary information technologies to permit prioritization and exploitation of large volumes of textual data without the need for prior human translation or transcription” (Report to President of the U.S., 2005, p. 396). Robert Ackerman (2006) noted that the OSC planned to assume the role outlined by the WMD Commission and serve as a center of excellence for information technologies, as well as its main purpose of producing OSINT and providing training at its academy to develop OSINT experts. Ackerman noted that the OSC wanted to serve a central role in acquiring and developing new information technologies for the IC:

> And, the center (OSC) will be working with the private sector to develop new techniques and technologies for open-source collections. The vast majority of the OSC's information technology work is outsourced to commercial companies,

> Naquin attests. These include integrators and companies with niche technologies such as large scale data exploitation. (Ackerman, 2006, para. 30)

Ackerman also noted that the OSC had a long wish list of commercial technologies that it needed to accomplish its mission and recounted comments from the former OSC director, Mr. Douglas Naquin. "When you're dealing with the potential universe of data, it's pretty daunting," Naquin asserted. "So one of the things that we look at is anything that will help us filter that information" (Ackerman, 2006, para. 33). Naquin specifically cited technologies such as filtering tools, machine translation, video filtering, and data mining as examples of tools necessary to deal with the vast amount of data available to the OSC.

Gregory F. Treverton, author of “The Next Steps in Reshaping Intelligence” published by the RAND Corporation, suggested that the IC was hard at work developing technologies for OSINT in 2005. He highlighted efforts at the CIA’s public-private technology firm, In-Q-Tel, at the IC’s Advanced Research and Development Activity (IARPA), and the Pentagon’s Defense Advanced Research Projects Agency (DARPA) as working on tools to mine large data sets. Treverton cautioned, however, that building tools and technologies for the sake of building do not address key issues if the tools are not built to match required or desired analytical outcomes (Treverton, 2005, p. 21).

The Need for Technological Solutions

Although the need for advanced information technologies to help with OSINT had been evident for decades, the realization that the IC required advanced tools and technological solutions to help solve issues in dealing with the vast amount of potential OSINT came to light in 2006, with the proclamation that the IC had not yet developed sufficient answers to the problems of the information overload. Codified into law, the

NDAA of Fiscal Year 2006 noted that “With the Information Revolution, the amount, significance, and accessibility of open-source information has expanded significantly, but the intelligence community has not expanded its exploitation efforts and systems to produce open-source intelligence” (PUBLIC LAW 109–163, 2006, section 931). Best and Cummings also argued in 2007 and again in 2008, that while the IC had finally reached consensus on the importance of OSINT, the IC was still in the process of examining key OSINT issues, including “…the state of development of analytic tools necessary to effectively and efficiently collect, sift, analyze, and disseminate a vast volume of publicly available information…” (Best & Cummings, 2007 & 2008, p. CRS-1). In 2010, the secretive CIA published a series of unclassified reports on the intelligence disciplines on their unclassified website (http//:www.cia.gov) and their first published article highlighted OSINT. The article highlighted that the vast amounts of potential OSINT available in the public domain presented a challenge that technology must help solve. A quote from the CIA’s article noted that “The sheer volume is daunting, and separating wheat from chaff requires skill, knowledge, and a reliance on sophisticated information technology” (INTellingence: Open Source Intelligence, 2010).

Technological Review

Chapter 3 reviews the implementation of select information technologies within the IC that aimed to improve how OSINT is produced and used by members of the IC. The constraints of this thesis, along with the often closed-nature of the IC, prevent an exhaustive review of technologies implemented. Numerous examples included in this thesis do provide the readers with an overview of the kinds of technologies, and their benefits to OSINT, framed within the steps of the IC’s intelligence cycle. The following

Chapter aims to serve as a catalyst to discuss the issues of technological diffusion within the IC, its processes, goals, and desired outcomes; in this case, how have implemented technologies thus far helped OSINT reach its potential as envisioned within the IC.

CHAPTER 3

TECHNOLOGICAL REVIEW

“There is no shortage of analytical tools being created, inside and outside the Intelligence Community.” (Gregory S. Treverton, 2005)

OSINT Technological Review

There are numerous tools and technologies designed to exploit the growing amount of information available within the public domain. The information revolution has spawned sophisticated tools and technologies that enable users to sort through, process, and analyze this amount of information in a systematic manner. Explaining past attempts to implement OSINT tools and technologies is the aim of this chapter.

Immense amounts of data and information are available for collection, processing and exploitation into OSINT. As outlined in Chapter 2, information technologies play a central role for IC analysts; no analyst could possibly collect, process, and exploit all potentially relevant OSINT that exists within the public domain. To maximize the value that OSINT can contribute to finished intelligence production, tools and technologies need to collect, process, and exploit information in a variety of ways. Technologies implemented to improve OSINT should provide IC analysts the ability to make OSINT useful to their analysis. As former DNI McConnell (2007) said about OSINT, the IC needs to "…have it available, to sort it out, to be able to touch it, to be able to examine it, to be able to have it useful in the context of the problems we're attempting to work…".

The IC requires a multitude of tools and technologies to separate the potentially valuable pertinent and relevant information from the multitude of information that exists within the public domain to produce OSINT. Like other sources of intelligence, OSINT needs to be examined for relevancy as well as validated for reliability. Proven, reliable OSINT that may hold answers to intelligence requirements need to be fully exploited to discover key information such as people, both known and unknown relationships, as well as discovering potential links within the data that are not readily apparent.

Current Technology Acquisition & Implementation Practices

Outside of centralized efforts to produce OSINT (which will be addressed in subsequent sections), the IC relies on a distributed, or de-centralized, approach, that is, contributions of OSINT from IC members for the benefit of all. This "gestalt" principle was outlined in the 2006 NOSE OSINT vision covered in Chapter 2, and expresses that the whole of OSINT produced through IC-wide efforts is greater than the sum of its parts (Jardines, 2006, p. 5).

The IC provides access to a range of information technologies to conduct business within the existing information architecture, mission specific tools and technology acquisition practices revolve mostly around agency-centric solutions, with each agency developing or acquiring IT to support their individual OSINT, and other intelligence, efforts. While this chapter solely focuses on past tool and technology applications aimed at OSINT, we discuss some potential updates to this IC-wide practice in Chapter 5.

Finally, IC IT requirements demand a tremendous amount of resources, with some estimates that agencies spend 25% of their National Intelligence Program (NIP) monies (IC CITE: Doing in Common What is Commonly Done, 2012, p. 2) on information infrastructures. Once tools and technologies are acquired and fielded within an agency's information infrastructure, the on-going costs to maintain and update technologies become an enduring financial commitment. New acquisitions of additional tools and technologies oriented toward improving OSINT, outside of investments in traditional intelligence mission requirements, may be beyond the reach of some IC agencies due to these long-term IT investments.

Moving forward, we begin by examining some of the previous attempts of the IC to implement tools and technologies that have application for OSINT, and potentially other intelligence disciplines, using the intelligence cycle as our framework to discuss where a particular tool or technology may provide solutions to OSINT deficiencies.

Overview - Technologies and the Intelligence Cycle

The intelligence cycle is the general scientific method or process used by IC analysts to produce finished intelligence. It is the generally accepted method used to answer intelligence questions and follows five important steps (refer to figure 1, Chapter 1).

We utilize the intelligence cycle to frame the discussion for the following sections which review past IC attempts of implementing tools and technologies with application to OSINT. In each of the following five sections, we begin by explaining each step of the intelligence cycle, and then examine the desired benefits that tools and technologies perform to assist IC analysts in sorting, filtering, producing, and ultimately making better use of OSINT to answer intelligence questions. Then we examine past attempts of the IC to implement tools and technologies to provide the better use of OSINT within finished intelligence production.

First step of the intelligence cycle - planning & direction. The first step of the intelligence cycle is planning & direction. This step requires analysts to examine the “assigned” or standing intelligence question, review currently available information, and to identify gaps, or unknown information, which would be helpful to providing a complete answer. Once gaps are identified, then the analyst can plan a strategy to assign appropriate IC resources to try and gather, or collect this information. To meet the ideas outlined in the first goal of the 2006 NOSE OSINT vision, this step would focus on efforts to survey or collect all known OSINT that may answer the question, then to continue to search for potential OSINT within the public domain to answer a specific question. Once OSINT was fully developed, then the analyst would turn to other sources of intelligence to fill in the remaining gaps.

Tools and technologies implemented for OSINT in the first step of the intelligence cycle should provide tools to manage known OSINT, as well as manage additional collection requirements that may be answered by it. When possible, these information requirements should be developed as close to classified requirements as possible, to make sure that OSINT is positioned to answer as many intelligence requirements as possible before classified resources are expended. Effective development and implementation of technologies during this step of the intelligence cycle are crucial to allowing the IC analyst to begin the process having access to, and fully considering existing OSINT resources before moving onto more scarce, classified sources.

The IC went right to work on initiatives aimed to improve this first step of the intelligence cycle. The IC identified the need to develop “a single open source requirements management system to balance resources against priorities…” (Best & Cumming, 2007, CRS-12). The DNI put forth this initiative in the first 100 Day Plan issued in 2007 (McConnell, 2007). Ackerman noted separately that the ADDNI/OS, Jardines, spoke about the requirement to merge the intelligence requirements systems within the OSC into one system: “We’re going to consolidate the process of collection requirements and the dissemination process.” (Ackerman, 2006, para. 7).

To this end, the IC developed and delivered an OSINT requirements system, entitled the Open Source Collection Acquisition Requirements – Management System, or OSCAR-MS. OSCAR-MS was defined in the Army Techniques Publication (ATP) 2-22.9 as “The primary open-source requirements management operational information and technical information database…” (Department of the Army, 2012, section 2-24, p. 2-5). According to ATP 2-22.9, OSCAR-MS:

> …is a Web-based service sponsored by the Office of the Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS) to provide the National Open Source Enterprise (NOSE) with an application for managing open-source collection requirements. OSCAR-MS links OSINT providers and consumers within the intelligence community… (Department of the Army, 2012, section 2-24, p. 2-5)

ATP 2-22.9 went on to further define the desired functions of OSCAR-MS that would support OSINT by:

- Providing useful metrics to understand OSINT requirements
- Allowing the digital indexing and tagging of submitted and completed open-source products to be searchable in the Library of National Intelligence
- Providing for local control of administrative data such as unit account management, local data tables, and local formats
- Allowing simple and flexible formats that employ database auto-population
- Using complete English instead of acronyms, computer codes, and other nonintuitive [sic] shortcuts
- Allowing linkages between requirements, products, and evaluations
- Enabling integration of open-source users for collaboration between agencies
- Reducing requirement duplication through customers directly contributing to existing requirements (Department of the Army, 2012, section 2-24, p. 2-5)

Although little additional information on the OSCAR-MS system is available, if designed in accordance with the identified key functions and intentions as above, and implemented within the IC in a system-wide update of collection practices, OSCAR-MS would go a long way in helping OSINT reach its desired place within the IC.

Second step of the intelligence cycle – collection. This step of the intelligence cycle, collection, is not the major challenge facing the IC; on the contrary, today's collection techniques may be the largest contributor to information overload for IC analysts. Collection technologies and techniques for OSINT are well documented within the literature for the most common types of data found on the internet, and in other forms of media.

Communication and information technologies have already played a prominent role in creating vast amounts of previously unavailable information. With this deluge of new sources of information, technologies that may improve the ways in which the IC collects information, potential OSINT, should focus on the automation of collection processes based on user selections and preferences, whether it be radio broadcasts, television, or information found on the WWW. Technologies should focus on decreasing the amount of time agencies and analysts spend in this step of the intelligence cycle.

The U.S. IC has longed realized the value of collecting of world-wide radio, and later television, broadcasts to be converted into OSINT. The FBIS was founded in 1941 to listen to, and transcribe AXIS media broadcasts (Shrader, 2005). This later expanded into the collection of newspapers, periodicals, publications, both in hard copy and later from digital sources. Information technology diffusion in the 1990s led to many newly available sources of on-line information. The IC established the COSPO in 1994 and its efforts were led by the CIA (DCID 2/12, 1994). The COSPO created a six node internet link to provide accesses to open source intelligence sources among six IC agencies, along with subject matter experts across the globe via email services (Betts, 1994). The

GlobalSecurity.org Website noted in 2014 that this system was called the Open Source Information System (OSIS).

Following the creation of the OSIS, the IC created the World Basic Information Library (WBIL) in 1997 (Kipp, 2005). The WBIL was created by using military reservists to build databases of military and other open source security-related information. The WBIL was hosted on the OSIS. Popular OSINT data sources of the time included selected FBIS reports, Jane's Defense military publications, and a database of over 900 International Journals, magazines, and newspapers, along with other valuable, defense related information culled from a variety of sources (Turbiville, Prinslow, & Waller, 1999).

Finally, the FBIS served as the core organization that was later subsumed by the establishment of the DNI OSC (Peak, 2005), and brought a well established technological collection capability, along with tried and true technological applications aimed to produce a wide variety of OSINT from world-wide sources. The collection of world-wide radio, television, internet, and multi-media information continues today, and the OSC is the still the IC's predominant producer of OSINT.

The internet. The OSC continues to follow established collection strategies of the past, as well as on the collection, monitoring, and processing of information from a number of Web sites, web blogs, newspapers, books, and other media sources. Due to the large amount of information available on the Internet, the OSC can not possibly collect all desired information. The OSC must concentrate on key sources that proved to provide valuable and reliable OSINT. With a small, but technologically savvy workforce, the OSC performs its assigned missions supplying the vast amount of OSINT for the IC.

With the distributed OSINT practices within the IC, IC analysts may have interests or requirements for OSINT that the OSC doesn't currently provide; plus agencies have responsibilities (and IC analysts) to collect and process OSINF into OSINT necessary to accomplish their unique requirements and assigned missions. The Internet provides almost an endless supply of information available for intelligence analysts and readers alike. IC analysts have the same accesses as the reader to the vast amount of information on the Internet; however, IC personnel follow additional security steps as required to conduct searches and before going to particular locations on the web. To perform a basic search, or to "Google" something, is the beginning of a search for information on a particular topic. This is an important step in the collection process, especially given that individual analysts are widely responsible to capture and create their own OSINT for use in answering key intelligence questions. Search engines have improved immensely over time with their advanced search algorithms. Popular engines today include Google, Yahoo, or Bing (Microsoft), amongst many others. For the growing number of sources of information on the internet, search engines have one thing in common: the search engine is the tool which helps find information, and is often used by IC analysts engaged in OSINT production.

However, there are limitations to the commonly used search engines, and that is they only search a fraction of the available information that exists on the Internet. Estimates are that only one percent of data available on the Internet are available as results on common search engines (Pagliery, 2014). There are special search engines that developed to troll the deep web, where the other 99% of the information resides. This vast amount of information on the Internet is not available for indexing by the most common search engines. One noted example of a special search engine to explore the deep web is Bright Planet®, which has reportedly been deployed within the IC for the last eight years. The Bright Planet® Web site www.brightplanet.com advertises multiple solutions for OSINT applications including deep web harvesting and preparation of the data for mission analytics (analysis), storage of harvested data, a deep web monitor that allows the user to use any browser to set up and create customized targets and keyword alerts on topics of the user's choice, and a real-time monitoring of Twitter (Bright Planet® Website, 2014).

The IC has focused interests and efforts in the development of specialized tools and technologies that help collect information from a variety of locations on the Internet. The CIA's private sector company, In-Q-Tel, is aimed at providing funding and research to technology companies that develop technologies of potential value to the IC. In-Q-Tel continues to make investments in companies aimed at tackling key issues with the collection of big data:

> Visible Technologies reportedly crawls over half a million web 2.0 sites a day, scraping more than a million posts and conversations taking place on blogs, YouTube, Twitter and Amazon. Attensity applies the rules of grammar to the so-called "unstructured text" of the web to make it more easily digestible by government databases. Keyhole (now Google Earth) is a staple of the targeting cells in military-intelligence units. (Shachtman, 2010)

For more information on how the CIA set up In-Q-Tel to invest in private sector information technology (IT) initiatives to help close the technology gap for the IC, see M. Belko's 2004 Air Force Institute of Technology 2004 Master's thesis.

Social media. Social media Web sites are another growing source of potential source of OSINT for the IC. One social media collection effort, entitled Argus, reportedly monitors foreign news media and other sources for early indications of impending events throughout the world. It was reported to monitor "…more than one million reports a day from nearly 3,000 sources in 21 major languages in 195 countries" (McConnell, "Overhauling Intelligence", 2007). The IARPA, the IC's equivalent program to DoD's DARPA, was also reported to be engaged in another OSINT-related program aimed at gathering digital data from sources such as "traffic webcams to television to Twitter" (Weinberger, 2011, p. 301). In 2013, an Air Force Foreign Area Officer offered some examples of social media aggregation sites that monitored trending topics, current events, and population sentiments, that were deemed crucial in the performance of his duties. He suggested that "properly integrating available social media exploitation and OSINT analytical resources is critical to being able to fully understand the geopolitical environment in a technology-driven society" (Sheets, 2013). A *Business Week* from article in 2013 showcased the IC's propensity toward exploiting social media for OSINT applications. The article claimed that the ODNI was sponsoring research in 14 universities in the USA, Europe, and Israel to see if popular social media and on-line data could provide indications of significant societal events using advanced analytics (Warner, 2013).

Internet – IC information distribution. By design, the IC built its internal information network technologies based on the standards and protocols used by the Internet. Using these common standards to build an information architecture provided the IC the ability to apply commercially developed technologies used for information management, discovery, and sharing. The IC created Intelink, the IC version of the Internet, in 1994 to support a "broad range of intelligence providers and consumers" (Intelligence Community Chief Information Officer, 2010). A. Dennis Clift, past President of the Joint Military Intelligence College, captured Admiral Studeman's assertions that the use of internet technologies was a boon to the IC in the mid-1990's:

> Application of evolving Internet technologies to intelligence applications in the form of Intelink has been a transcendent and farsighted strategy. Its future application requirements parallel those of the global Internet, so that there is the expectation that, for continuing modest investment, intelligence can continue to ride the wave of Internet growth, with commensurate access to amazing and relevant commercial off-the-shelf (COTS) developments. (Clift, 2003, p. 75)

Intelink provides the network for the sharing of all types of intelligence information across the IC, including OSINT. Intelink provided many tools that mirror commercial developments including social media, video repositories, blogs, instant messaging, document storage and collaboration work spaces, and many more (Intelligence Community Chief Information Officer, 2010). The Intelink also hosts IC member databases and repositories of OSINT. One example, the Harmony Database, is a collection of document and media exploitation efforts, both classified and unclassified, and serves as a national repository to the Defense Intelligence Enterprise and the IC for translated foreign documents, and captured documents and media ("2009 U.S. Army Posture Statement Document and Media Exploitation," 2009).

One company recognized that the IC and USG operated many distributed and disparately located and related agency-centric databases to house intelligence and information. Chiliad built a virtual database consolidation tool for parts of the IC, and this tool is reportedly in use by elements of the FBI and the DHS (Yasin, 2013). The Chiliad Discovery/Alert tool as referenced on the Chiliad Website, www.chiliad.com, eliminates the need to physically combine databases, instead relying on the installation of nodes at each original data location. These nodes then work together to create a virtual consolidated data center, which allows analysts to search against both structured and unstructured data sets across all distributed databases. This virtual linking of disparate databases could help solve many issues related with distributed databases found across the IC enterprise.

The IC also utilized the public Internet when establishing the OSC's main Web site, www.opensource.gov. This Web site is for authorized users and provides access to the OSC's full production database of OSINT, along with other sources of information such as newspapers, magazines, databases, and on-line information subscription services purchased for use by IC analysts. Mr. Al Tarasiuk (2009), then the Chief Information Officer (CIO) of the CIA, now the DDNI and chief IC CIO, recounted the OSINT menu of information found in the OSC Web site. He noted OSC successes in providing 128 databases, including the Web of Science, to 20,000 authorized users representing all IC personnel, including uniformed, civilian, and senior policy makers. In addition to the commercially provided content from OSINT producers such as ProQuest, Janes, and

Oxford Analytica, the Web site rehosts open source materials from 115 other USG entities. The site also offers videos from over 50 foreign TV stations. In addition, the Web site pushes out selected OSINT streams to a variety of internal messaging systems in use throughout the USG (Tarasiuk, Remarks at the 2009 GEOINT Symposium, 2009).

Third step in the intelligence cycle - processing & exploitation. The third stage of the Intelligence Cycle is the processing and exploitation of collected information into a useable form, and for the information to be considered OSINT. With the vast amounts of and the variety of the types of information available for collection, both structured and unstructured data, tools and technologies benefits to this step of the intelligence cycle strive to make future analysis possible. Once OSINF is collected, and continues to this step of the intelligence cycle, the conversion is largely finished, and is now considered OSINT. This step involves extraction of key attributes of the information including the source, date, time, content, actors, metadata, etc.

The technologies employed during this step of the intelligence cycle are essential to making sense of the details found within the information, along with its conversion to a usable form as OSINT. Advanced technologies have positively impacted the IC's ability to produce OSINT. The automated processes these technologies perform are essential to the IC understanding, the gleaning of salient information, and discovering previously established relationships within large sets of data. In essence, tools and technologies applied toward efforts in this step of the intelligence cycle for OSINT may provide the most impact when making efforts to "connect the dots" within the seemingly endless amount of OSINT now available.

Text-mining. The IC has implemented text-mining technologies to parse through collected intelligence and extract key aspects of the information within to be used for analysis, step four of the intelligence cycle. Some examples of the types of information that is marked for later analysis include people, places, things, numbers, titles of events, amongst others. Text mining has been a long established process within existing IC information databases. Cade Metz (2003), writing for PC Magazine, wrote on the growing use of the U.S. government in implementing text mining software to enable analysts to connect the dots. Metz (2003) noted that text-mining is one of the tools that elements within the IC are using to search through multitudes of unstructured text to pull out useful information, or to infer relationships among the data that are not explicit. Text-mining can locate words and phrases much like using a regular search engine, however, "…the software can identify relationships, patterns, and trends involving words, phrases, numbers, and other data" (Metz, 2003, para. 4).

Another company partially supported by In-Q-Tel is Recorded Future. Recorded Future performs metadata extraction from web pages, capturing such information as the people, places, and activities mentioned within the text. It then examines when and where these events took place and try and determine the tone of the source. The program reportedly then applies "…some artificial-intelligence algorithms to tease out connections between the players" (Schactman, 2010, para. 11). These technologies interpret the raw data that comes from both structured, and unstructured data and exploits the entities, or variables that can be used later in intelligence analysis.

One of the fundamental problems with the deluge of available and exploitable information to be used in creating OSINT is finding and extracting relevant, useful information. Technologies geared toward getting at the data, discovering relationships within the data, etc. Data mining tools are designed to do just that. The IC has implemented some forms of data mining technologies. Prior to becoming the OSC, FBIS reportedly realized success in data mining efforts through their partnership with IBM. IBM tailored the data mining algorithms in collaboration with FBIS and:

> …generated data-mining algorithms uniquely tailored to FBIS's needs, along with new search and correlation technologies that have let the organization achieve a seven-fold increase in output with half the staff. The Web crawlers produced by IBM and tailored to FBIS's needs far surpass Google in efficiency. (Treverton & Gabbard, 2008, p. 25)

The OSC utilizes data mining, along with a combination of other tools such as link analysis, visualization tools, and machine translation, in producing OSINT (R. Ackerman, 2006). Multiple IC agencies since 2005 have reportedly implemented data mining tools or technologies to aid in "making sense" of collected information. Data mining uses mathematical formulas to determine unknown patterns, trends, relationships from disparate data. Data mining tools have been especially helpful to law enforcement and counterterrorism in hunting and tracking down terrorists by agencies such as the Federal Bureau of Investigations (FBI), and the Department of Homeland Security (DHS) (Mohammed & Goo, 2006).

Another tool aimed at "connecting the dots" and available to select users in the IC is Palantir. The Palantir company Web site at www.palantir.com claims that Palantir aims to provide customers ability to consolidate all available organizational databases and to "integrate disparate data from disconnected data silos at massive scale…" and to

"…search through every shred of enterprise data at high speed, pull out significant intelligence, and perform intuitive, multi-dimensional analysis to reveal unseen patterns, connections, and trends" (2014). Palantir reportedly received financial support from In-Q-Tel, and the CIA reportedly served as its only customer for several years (Greenberg & Mac, 2013). Greenberg & Mac (2013) of *Forbes* reported that Palantir has become the "go-to company" for mining massive data sets for intelligence operations. Palantir also received high praise from former CIA director George Tenet, who was quoted as saying that he wished the CIA had a tool of its power before 9/11 (Greenberg & Mac, 2013).

Foreign language tools and translators. Realizing that a preponderance of the potential OSINT available to the IC does not exist in English, Congress mandated the creation of the National Virtual Translation Center (NVTC) after 9/11 to provide timely and accurate translation of foreign intelligence for all elements of the IC. Their mission is designed to augment foreign language capabilities throughout elements of the IC and the military. The NVTC receive requests for translation services and are able to process and translate a variety of documents, audio files, videos, handwritten notes. Their efforts produced translations for all levels of classification, from unclassified to Top Secret. The NVTC utilizes speech to text and machine translation to determine which translations require human translation. Although part of the solution in providing foreign translation services for the IC, there are costs involved to those requesting translation services (Egan, 2005).

Non-linguist IC analysts have also used a number of commercial available machine translation services. One commonly used commercial translation tool is Google Translate, available on Google's Web site translate.google.com. There are a number of others available on the Internet including www.babelfish.com, and www.bing.com/translator to name a few. Analysts who require translation support to review information can cut and paste foreign language characters into a translator program from one of over 50 available languages and receive computer generated translation results. Although the provided translations often fall short of providing a complete understanding of the foreign language material, an analyst can use this translation as a starting point to develop a general sense of whether the information holds value to a particular intelligence requirement. This partial solution to translation can often used to decide whether to invest time and resources converting the information into OSINT.

Fourth step of the intelligence cycle – analysis. This step of the intelligence cycle requires tools and technologies that will allow IC analysts to make sense of the acquired, collected, and converted information now considered OSINT. This step focuses on building knowledge about a particular topic or question, and judging new data in relation to existing data to make analytical judgments, or assessments.

Technological solutions applied to the preceding steps of the intelligence cycle aim to automate some of the required processes, and provide key details found within the data. One could argue that technologies applied in the preceding steps should aim to provide analysts the ability to spend the most time during this step of the intelligence cycle. Tools and technologies implemented to aid intelligence analysis provide ways to organize, view, discriminate, or visualize available information in a variety of ways. Some argue that tools and technologies developed for analysis are less critical, that humans must always be in the loop. To this end, this examination focuses on a few emerging tools and technologies that have presented IC analyst's additional ways to look at the vast amount of OSINT available.

Commercial geography solutions. Commercial geographical information system technologies are now common. Tools like Google Earth and Streetview, provide geographical solutions that were previously only available from national collection assets. Analysts can plot geo-tagged OSINT on customizable maps to aid in the visualization and analysis of the data. Deployed military units can utilize Streetview data and maps to plan operations, to minimize their classification (Williams, 2011). Commercial imagery can also used to produce OSINT products, and for some applications in protecting national technical means, may be a necessity when sharing information with foreign partners, and other un-cleared mission partners such as non-IC personnel, and law enforcement officials. The ability of the analyst to perform some of these functions within their established work-space can reduce the amount of time it takes to produce such products, and reserves the use of other more scarce IC collection resources.

Social networking and collaboration. Wright (2008), Howard (2010), and Thomas Wailgum (2008) noted that the IC has created or adopted numerous social networking and collaboration tools aimed at fostering collaboration among IC analysts. Intellipedia, the IC's secure version of Wikipedia, was created in 2006. The IC also developed A-Space which was based on social networking sites such as MySpace and Facebook, which allowed IC analysts to build collaborative environments aimed at improving intelligence analysis. While not developed to address the production and sharing of OSINT, these on-line communities are often used to share pertinent information to self-selected groups of analysts. These tools can be valuable to particular IC analyst’s social groups, especially when sharing the latest OSINT. These tools are especially important once members of the group post, or share, selected OSINT on a particular topic or issue.

Clustered search results. Some analysts within the IC use a clustered search engine named Vivisimo – Velocity (now IBM’s InfoSphere Data Explorer) to improve individual search results across the distributed IC information repositories, as well as across the classification domains. Velocity provides a starting point for analysts to begin a search and returns results that are automatically organized and combined into clusters, or folders to organize the results ("Vivisimo Gets NSF Data Contract For Homeland Security," 2003). In 2011, Vivisimo released a press release on the raid on Osama Bin Laden’s compound and to promote their contributions to the IC. The vice president and general manager of Federal for Vivisimo, Bob Carter, asserted that:

> The defense and intelligence communities recognize the need to improve the 'signal-to-noise' ratio for large disparate data sets as a way to achieve true all-source analysis and deliver timely, objective, and actionable intelligence to our senior decision makers and war fighters. Defense and intelligence analysts rely on Vivisimo to effectively pinpoint critical information that is being produced both within their network as well as public information coming from social media and other Internet sources. ("Discovery of Osama Bin Laden Result of Improved Information Sharing Amongst Intelligence Analysts... -- WASHINGTON, May 5, 2011 /PRNewswire-USNewswire/ --," 2011)

Social Bookmarking. Ackerman, et al. (2007) reviewed another IC technology that relies on crowd-sourcing to identify key words and “tags” of various sources of intelligence. They discussed a new IC tool based on the commercial concepts of del.icio.us and Flickr.com, known as tag|connect. “This tool enables analysts to categorize and archive information they collect for later retrieval, while at the same time engaging in collaborative sensemaking [sic] through a dynamic framework.” (Ackerman et al., p. 679). IC users of tag|connect are charged to “tag” sources of information, including OSINT, with multiple keywords they deem appropriate to categorize or describe each report. This aids both the individual user as well other analysts within the IC to discover items of interest, not just relying on common search methods, but on general concepts of the content contained within. For OSINT, analysts could immediately find examples of tagged OSINT that may be important to their particular intelligence question. By following particular concepts and key words on a particular topic, tag|connect may expose analysts to information not previously considered. The goal was to lead to a different way of tracking down produced intelligence, including OSINT that may lead to greater exposure of information that may be pertinent to particular groups of IC analysts.

Visualization tools. Analytic tools found within the data and text mining technologies discussed in the previous section attempt to make sense of the data from a users search. The outputs of Data mining, for example, report previously unknown relationships between the data. These relationships could be between people, places, or things. Analytical tools to help decipher these relationships are essential to making sense of the new-found relationships, and are key to effectively using the results of Data mining efforts.

One particular analytical tool that has reportedly been widely implemented within the IC is Analyst Notebook. According to the IBM Website, www.ibm.com, i2 Analyst's Notebook:

> …is a visual intelligence analysis environment that can optimize the value of massive amounts of information collected by government agencies and businesses. It allows analysts to quickly collate, analyze and visualize data from disparate sources while reducing the time required to discover key information in complex data.

Analyst's Notebook is also advertised to "Rapidly piece together disparate data into a single cohesive intelligence picture" (IBM Website, 2014).

Fifth step of the intelligence cycle – dissemination. This step of the intelligence cycle would ensure that all OSINT produced is discoverable by all IC analysts and likely intelligence consumers. There is no real purpose in producing OSINT if not to increase and improve the IC's use of publicly available information to produce finished intelligence. The distributed production model for OSINT within the IC which relies on the wide-spread production of OSINT from its members, not just from the OSC, thereby establishing known OSINT to ensure that the IC doesn't spend scarce time and resources producing what is already known.

Tools and technologies involved in the dissemination of OSINT should focus on the maximum dissemination of produced OSINT to IC analysts, and should consolidate known OSINT data sources across the IC enterprise to allow sophisticated tools and technologies to perform the functions for which they are designed. We have discussed some efforts of this so far in this examination.

IC information sharing initiatives resulted in the consolidation of OSC produced OSINT in a single Web site at www.opensource.gov, which contains both produced OSINT, other information sources, and on-line shared accesses to subscription-based services. OSINT is also available on Intelink either through typical search engines or through navigation to one of the many IC OSINT databases distributed throughout the IC.

In addition to the OSC repository of OSINT and other streams of information, most internal IC message dissemination systems include some sources of OSINT. As has been previously established, different IC agencies have developed or acquired IT systems to be used in the distribution of intelligence reports, including OSINT. One tool, in use by the Armed Forces and by some in the IC, is called the Distributed Common Ground System (DCGS). DCGS-A, the Army version, was developed to connect deployed combat troops with the Intelligence community through instant information sharing, and shared intelligence databases (DCGS-A Website, http://dcgsa.apg.army.mil/, 2014). DCGS-A also combined Analysts Notebook, the social network analysis tool previously explored, as a specialized analytical tool (IBM Web site, 2014). The Navy uses a "cross-domain messaging solution" from Northrop Grumman called Smart.neXt. This system is deigned to operate across all domains within the IC on a single system in which users can subscribe to, and receive published information in a timely manner (Goodwin, 2014). Wailgum (2008), past senior editor for CIO.com and CIO magazine, noted that the CIA fielded Trident in 2007 which connected CIA analysts with about a dozen or so data sources. In addition to allowing analysts to manage the voluminous amounts of incoming data, Trident provides other capabilities, such as search tools, information extraction, link analysis, mapping, and visualization. These disparate IT systems combine a multitude of disparate data sources into a single message dissemination system, including OSINT. The provided examples are representative of the types of systems in use by various members within the IC.

Some of these systems have tools that help analysts perform a variety of functions, mostly to aid analytical efforts, as outlined above in step four of the intelligence cycle. Access to a particular tool or technology is heavily dependent on an analyst's affiliation within a particular agency, as IC agencies acquire these tools and technologies through distributed, agency-centric technology acquisition processes. While these tools and technologies aim to provide access to available intelligence and information sources, not all sources of OSINT within the IC are included in all internal message distribution systems. Many OSINT repositories exist in distributed locations throughout the information networks of the IC and its agencies, requiring analysts to navigate and search databases in disparate locations within the IC information networks.

One promising technological initiative that was created in response to DNI initiatives is the Library of National Intelligence (LNI). The LNI allows IC analysts and collectors to discover already produced streams of published intelligence information, including the sources used in the finished production, whether IMINT, SIGINT, or OSINT. This system addressed key issues outlined in ICD 501 on the dissemination of intelligence and intelligence related products within the IC (Tarasiuk, Remarks at 2009 GEOINT Symposium, 2009).

Conclusions

There has been notable progress by the IC in the implementation of tools and technologies aimed to improve how OSINT is collected, processed and exploited, produced and used. The IC adoption of common internet protocols to form the backbone of its information systems was notable as it allowed the adaption of commercial sector information technologies for use within the IC. Outside of IC fielded tools for social networking, or collaboration, however, access to more sophisticated tools and technologies varies depending on where an individual analyst works – individual analyst's experiences and results will vary. OSINT, however, is now provided in multiple intelligence streams, found in multiple tools and technologies, and published in a variety of locations within IC networks, and in the case of the OSC Web site, on the public internet. The amount of OSINT available to today's intelligence analyst would surpass the amounts thought possible by OSINT advocates just two decades ago.

This chapter chronicled IC attempts in harnessing tools and technologies that were aimed to improve the ways OSINT is produced and utilized within the IC. When examined, several questions need to be explored. What processes and procedures are used within the IC to determine best technological practices for each step of the intelligence cycle? What feedback mechanisms ensure that the most valuable tools are implemented that address key OSINT issues? What mechanisms exist for tools and technologies to find widespread diffusion and implementation within the IC? What other commercially available information tools and technologies are available that have not been examined? Although this chapter reported quite a few examples of progress towards solving some identified OSINT technological deficiencies, reviewing the past implementation of tools and technologies alone may not provide all of the answers to the central question of this thesis. Chapter 4 will examine many system-wide limitations and challenges faced by the IC to realize its goal to make real gains in OSINT.

CHAPTER 4

INTELLIGENCE COMMUNITY CHALLENGES AND LIMITATIONS

Introduction

Despite the numerous attempts to improve OSINT practices and procedures within the IC, including the implementation of tools and technologies, the IC still faces many challenges. This chapter aims to present some of the reasons that technological solutions alone may not hold the answer to systemic change for OSINT within the IC. Other, key aspects of the IC may present obstacles that if left alone, or not addressed during the implementation, will continue to diminish future technological advancement and may inadvertently build road blocks for OSINT within the future IC.

Developing and implementing appropriate technologies aimed at solving OSINT challenges within the IC have met a number of challenges. Technologies largely perform tasks or improve processes for which they are designed. However, implementation within the larger socio-technical system introduces pressures from within the system that impede the desired effects of tools and technologies. The technologies reviewed in Chapter 3 showed the application of tools and technologies employed by the IC to address issues in more effectively harnessing the utility of OSINT within finished intelligence production. The application of tools and technologies within the IC have contributed to more access, opportunities, and efficiencies toward reaching goals outlined in the 2006 NOSE OSINT vision, and were aimed at solving challenges posed by the changing global threats, the globalization of information, and the exploding amounts and new sources of global information.

However, numerous system constraints or limitations have been identified that may impede substantial gains for improving OSINT within the IC. These issues include aspects such as how the IC is comprised, the leadership, the culture, the people, the processes, and the external influences that are sometimes at odds with, or sometimes present a barrier to, the full realization of OSINT's benefits within the IC enterprise. Some themes in this chapter present themselves as new; some are decades old. In any case they deserve to be examined. The examples provided herein are at least a starting point to explain important system constraints and limitations that may help answer why technologies have not yet fixed OSINT, and have prevented the IC from producing system-wide, tangible improvements.

System Constraints

Fiscal constraints. As a whole, the IC-wide information technology architecture is immense and imposes great costs amongst IC members. The existing model of agency instituted information technology (IT) acquisition and legacy IT solutions continues to exert fiscal pressures on the ability to individually acquire and implement technological solutions for OSINT. INSA estimated in 2012 that spending on information technology across the 17-plus agencies in the IC could "…be as much as 25% of the National Intelligence Program (NIP) funding not including IT funded as part of other program line items." (IC ITE, Doing In Common What is Commonly Done, 2012, p. 2). With the changing technological landscape, and the pressures to stay up to date with current technological advancements, the current practices focused on agency-centric solutions leaves little additional resources for agencies to make continued investments in the latest OSINT tools and technologies. In addition to meeting individual agency technology needs to help improve OSINT activities, agencies must also allocate funding in the maintenance of legacy technology systems, systems designed to interface with specific customers and services, as well as in providing the necessary tools for completion of internal tasks an long-term, more traditional intelligence missions. In sum, the financial obligations involved in the conduct of normal IC operations are enormous; allocating funds specifically designed to acquire new tools and technologies for OSINT may prove a long-standing impediment.

Leadership. Although the DNI was created as the centralized leader of the IC, his authorities to impact the operations and internal missions of IC members is limited by the powers afforded the office. Hamilton Bean (2007), assistant professor in the Department of Communication at the University of Colorado, Denver, noted that the future of OSINT will become whatever the DNI makes it be, based on personal communications with the former NIC Chairman, John Gannon (p. 241).

Following recommendations made by the WMD Commission (Report to the President of the U.S., 2005, pp. 379-380) to appoint institutional champions for OSINT, the DNI did define OSINT as important early in his tenure, and made key structural changes called for within the body of reforms, namely the establishment of the OSC and the previously mentioned Chief IC OSINT advocate, the ADDNI/OS. The DNI also issued ICD 301 (2006) which established OSINT guidelines for the IC, rescinding the previous efforts of the IC Open Source Program. However, the DNI’s actions could only establish OSINT as an important issue and to institute system-wide initiatives to promote its use. As the centralized leader of the IC, the DNI could not control all institutional, cultural and structural constraints that would ultimately determine (or possibly undermine) OSINT’s direction within the IC.

The DNI did receive expanded fiscal authorities over funding streams within the IC, unlike the previous leader of the IC. Statute authority provided the DNI with a significant amount of authority over the IC’s budget development and ensuring the effective execution of that budget. The DNI is charged with overseeing the NIP, formerly known as the National Foreign Intelligence Program. This funding provides the resources needed to develop and maintain intelligence capabilities that support national priorities. A large portion of the funding for members of the IC, however, originates in the DoD’s Military Intelligence Program (MIP). The MIP funds the specific intelligence needs of the DoD and tactical forces. The MIP is controlled by the Secretary of Defense, and the DNI assists in the development of the MIP (DNI, “U.S. National Intelligence”, 2013). The DNI controls IC-wide initiatives, develops standards, and demands accountability for results toward these goals. However, the DNI does not determine how each IC agency funds individual OSINT efforts outside of NIP funding allocations.

The ODNI is faced with complex financial decisions, completes annual budgets, along with five year budgets that plan the complex operations of the IC. Bean (2014) noted that the DNI charter imposes spending caps on system-wide technology acquisition, and large initiatives may require congressional approval. The establishment of Chief Technology personnel within the ODNI faced similar limitations on what can be implemented across the IC such as common data standards through the use of ICD’s, and through funding allocation. The DNI did launch initiatives in 2012 aimed at overhauling the IC Information Technology Enterprise (IC ITE). Although this initiative is not specific to only improving OSINT within the IC, these initiatives may aid in understanding the future direction for OSINT within the IC. This initiative will be further discussed in Chapter 5.

Despite the new emphasis on OSINT, and the statutory authority that rests within the office the ODNI, the DNI's IC budgetary and governing authority, by itself, was not enough to permanently institutionalize OSINT within the IC to achieve the goals outlined in the 2006 NOSE OSINT vision. The de-centralized "consortium" of IC agencies went about conducting OSINT largely as before. Bean (2014) recounts the former director of the OSC Naquin on the lack of institutional progress for OSINT "…we have not made great progress toward an IC-wide Open Source Enterprise." (Bean, 2014, p. 44).

Culture. IC cultural limitations may pose the largest obstacles for OSINT in realizing the goals outlined in the 2006 NOSE OSINT vision. The following sections review some common issues noted in the literature in regard to the challenges that still limit real OSINT gains within the IC. Some have argued that the IC still reflects similar processes, structures, and procedures of the past, and changes in the global threat environment, the globalization of information, and the growth of information technology did little to update how the IC as a whole changed its ways in regards to OSINT. Alfred Rolington (2007), former Chief Executive Officer of Jane's Information Group, noted that neither the Internet nor the end of the Cold War have been fully integrated into the thinking and practice of many of the traditional intelligence organizations (Rolington, 2007, p. 740).

Secrecy. Despite the consensus that OSINT is of growing importance to the IC, a bias still exists within the IC toward the reliance on, and utilization of classified sources in answering key intelligence questions. It's not that most IC members don't value OSINT, it's that OSINT means different things to different people and institutions. Bean (2014) noted that former OSC director Naquin related that the IC viewed their core missions, traditionally secret or clandestine in nature, as easier to quantify in their impacts to the IC mission, which ultimately reinforces an agencies orientation toward secrecy vice openness. OSINT in essence is an "outsider" to the institution charged with collecting and interpreting sources of classified information, and aligned with Lanheman's (2010) assertions that a single institution, in this case the IC, can't perform both a secret and an "open" mission. Best and Cummings (2008) echoed these ideas in the 2008 version of "Open Source Intelligence (OSINT): Issues for Congress", establishing that OSINT has finally gained acceptance within the IC, however, the inherent value of OSINT was still up for debate amongst the member agencies:

> They disagree, however, over its value relative to that of clandestinely-collected secret information, and thus the amount of time, attention, and resources that should be devoted to its collection and analysis remains in dispute. (Best & Cummings, 2008, p. CRS-2)

Despite the centrally led charge to improve OSINT within the IC, Bean (2014) also captured former OSC director Naquin's reflections that the OSINT movement had done little to fundamentally revise underlying institutional logic and commitments to OSINT at the expense of clandestine intelligence:

> Although there has long been talk that Open Source can provide a 'safety

> net' and might be 'good enough' on its own for certain issues, I never observed a willingness during high-level budget discussions to trade even small pieces of more traditional intelligence capabilities for investment in more comprehensive collection and analysis of open sources. It's not that such a scenario is inconceivable; it would just represent a major paradigm shift for the Intelligence Community. Such a trade would be a bellwether in the evolution of Open Source as an intelligence discipline. (p. 46)

The INSA Rebalance Task Force's white paper entitled "Expectations of Intelligence in the Information Age" (2012) warns that the IC needs to be prepared to grasp OSINT opportunities to fulfill its national security charter, and stated that:

> Today, the United States Intelligence Community (IC) still lives largely in the world of secrets defining intelligence; tomorrow, it will either embrace a new understanding of intelligence and knowledge or risk marginalizing analysts from this century's knowledge revolution and hence fail to serve policy makers as well as possible. (INSA, Expectations, 2012, p.1)

Future successes in the production of OSINT may also produce additional challenges that may necessarily produce more secrecy in the future. OSINT derived from sophisticated tools and technologies, or derived from a combination of advanced technological methods that provide the IC unique capabilities, accesses, or insights, may require that the results of such efforts be classified for protection of sources and methods, a key component in establishing classified information. Charles S. Clark (2012), Senior Correspondent for Government Executive, noted comments by Carmen Medina, a former director of the CIA's Center for the Study of Intelligence and co-author of the 2012 INSA

White Paper “Expectations of Intelligence in the Information Age”, where Medina said that that future data itself may not be classified, but rather that the methodologies for analyzing data may be. Bean (2014) also reflected this sentiment with revelations of the former OSC director Naquin, recounting that:

> One of the ironies of working in Open Source Intelligence is that the better we got, the less we could say about our successes. We did enjoy several notable successes that garnered kudos from leaders and stakeholders both inside and outside the Intelligence Community, but given the nature of these stories I cannot be specific. (2014, p. 52)

Over-classification is another problem that could be addressed through the use of more OSINT. Alex Young (2013), staff writer for the *Harvard International Review*, wrote in “Too Much Information: Ineffective Intelligence Collection” that systematic cultural issues within the IC on classification issues may be contributing to the over classification of information. Officials who over classify intelligence information see little to no penalties; while the system is set up to penalize officials who misclassify the smallest amount of secret information. The system creates the necessity of over-classification in favor of secrecy, and therefore, may devalue the contributions that OSINT may make within the IC (Young, 2013, pp. 24-27).

Lack of real consensus on OSINT. In spite of the prognostication of Best and Cummings in their 2007 and 2008 Congressional Research papers “OSINT: Intelligence Issues for Congress”, the IC still lacks real consensus on the value and importance of OSINT. Individual agencies ultimately determine their own value of OSINT, and dictate policies, the emphasis on use, along with the commitment of effort and fiscal resources.

This lack of consensus amongst IC members on OSINT's inherent value, especially when the IC counts on the distributed contributions of its members (outside the OSC), ultimately undermines one of the key goals outlined in the 2006 NOSE OSINT vision, and means that the sum of OSINT for the IC may in fact not be greater than its parts. In other words, the value, use, and commitment to OSINT vary across the IC.

IC members also view OSINT from different perspectives. One view is that OSINT is an intelligence discipline in and of itself, thus the acronym OSINT, or open source intelligence. OSINT has been loosely used over the years to refer to open source intelligence, and have loosely established it as one of the intelligence disciplines. The North American Treaty Alliance (NATO) published the NATO Open Source Intelligence Handbook under the direction of General W.F. Kernan. This handbook was designed to outline "…a systematic approach to OSINT exploitation" (Kernan, 2001, p. I). The U.S. Army (2006) published a temporary Field Manual (FM) 2-22.9 entitled "Open Source Intelligence" (Fast, 2005), which was later superseded by the publishing of an "Army Techniques Publication" 2-22.9 in 2012, with the same name (Department of the Army, 2012). The ADDNI/OS referred to OSINT as an intelligence discipline, noting that it should be used as the source of first resort. The U.S. Congress highlighted this position in The NDAA of Fiscal Year 2006 and referred to OSINT as intelligence discipline (2006, Sec. 931, para a.3). These are just some examples of how different actors within the IC and the DoD viewed OSINT.

The other prevailing view is that OSINT is primarily a collection discipline, albeit an important one to focus on. Kimberly Saunders (2000), a former student at the Royal Military College in Canada, tracked the views of Canada and the USA of OSINT over history in her Masters of Arts Thesis, “Open Source Information: A True Collection Discipline”. Saunders concluded that “A true open source collection discipline should be implemented, putting the collection of open source information on the same level as the other collection disciplines.” (p. 216). The former DDNI for collection, Mrs. Mary Margaret Graham, made comments at the first 2007 DNI sponsored conference on Open Source that from her perspective and from the consensus of the DNI who championed the establishment of the NOSE, was that “…open source is a discipline of collection” (Graham, 2007).

OSINT has not only competed for consensus in regards to its emerging importance to the IC, it has done so within a system whose members and leaders have failed to even view OSINT with the same, consistent definition. Examining the IC and its composition, there is a lack of consensus among member agencies, and by individuals, on the inherent value or definitions of what OSINT means to each. It is no wonder that the OSINT issue is complicated, as views among IC leaders, member agency leaders, and amongst individuals can and will vary widely across the IC enterprise. These competing views should be confusing to the reader; imagine the mixed signals that individual IC agencies discern from IC leadership on the status of OSINT within the IC.

Possibly recognizing the prevailing and differing definitions of OSINT, Bean (2007) asserted in his arguments that OSINT is both an intelligence discipline and a source of information, among other things. He noted that OSINT is a symbol within the IC, “More importantly, OSINT is also a symbol whose meaning and uses are negotiated by government officials, policymakers, and business leaders to support their respective agendas" (p. 246). The future of OSINT and how it is defined within the IC may hold key insights into which direction OSINT takes in the future.

Risk aversion. Adopting OSINT as the source of first resort posed many issues for the IC. IC-wide initiatives focused on information sharing and the integration of all types of intelligence to ensure that analysis is fully informed by the available information. To suggest that OSINT be used as the source of first resort, to be used first in intelligence analysis, largely leaves out the prescriptions for how this can be accomplished within the long-established analytic processes and practices of the IC, and run counter to integration initiatives. The 2006 NOSE OSINT vision suggested that OSINT could often satisfy 80% of the intelligence requirements, and that the remaining 20% of requirements could be focused within the secret intelligence disciplines scarce resources. While this sounds appealing, it ignores basic analytic principles used by all-source analysts. It should also be noted that the 80% estimate often asserted in regards to OSINT must be referring to the intelligence produced by all-source analysts, who regularly include information from a wide variety of sources of intelligence in their analysis. To assert that 80% of all SIGINT, or MASINT, or other sophisticated technical and human collection means could be satisfied through open sources seems to be divorced from reality.

The IC operates a risky enterprise and intelligence failures have dire consequences. It is not surprising that the IC continues to make slow, calculated decisions concerning necessary reforms. Changing institutional and analytical procedures is a risky proposition. Current leaders within the IC do not want to be held responsible for sweeping major reform efforts that fail to predict the next attack on the U.S., or other major global crisis because they were in the middle of implementing revolutionary IC-wide changes in regards to OSINT. Intelligence failure is a proposition most leaders, and the USG, want to avoid. Minimizing risk within the IC will continue to thwart major reform efforts that may improve OSINT's production and use within the IC. A RAND study published in 2008 noted that the:

> The Intelligence Community has a long history of commissioning the development of knowledge engineering and knowledge discovery techniques to address the issue of critical analysis and "strategic surprise," but little of this work has seen actual service. (Teverton & Gabbard, 2008, p. 24)

Distributed production of OSINT. Another consistent concern noted for OSINT lies in the practice of the distributed OSINT production responsibilities assigned to members of the IC. Senior IC officials have made the assertion that each IC agency's intelligence analysts should produce OSINT that meets individual agency requirements, and the production of OSINT should be performed by subject matter experts, such as all-source analysts who rely on the totality of intelligence sources in their finished intelligence production. This idea was espoused in the 2006 NOSE OSINT vision as "Gestalt" – the notion that the whole of OSINT produced by members of the IC is greater than the sum of its parts. The model related that everyone within the IC should collect, process and exploit pertinent publicly available information, or put more simply, produce relevant OSINT to their particular mission requirements. The IC would, in theory, benefit from the collective production of OSINT across the enterprise, with all produced OSINT shared by all. However, there are some basic issues with the premise that all-source analysts, subject matter experts, or collection-oriented analysts should largely produce their own OSINT. We examine some of these issues below.

IC analysts at all agencies may not be particularly well-suited to perform the production of OSINT within their current duties and missions. All-source oriented IC agencies already have challenges in that assigned analysts are focused on the integration of all intelligence disciplines to answer questions for their customers, not on the production of one kind of intelligence (OSINT). While all-source analysts at these agencies are commonly recognized as subject matter experts in their field, their focus is on the integration of all sources of intelligence to answer key intelligence questions, and to point out collection gaps from the various intelligence disciplines that need answered to be able to answer at-hand or future intelligence requirements. In short, the production of all-source finished intelligence revolves around analysts consuming large amounts of already produced intelligence and fusing it together into a coherent assessment that answers key intelligence and research issues, not around the production of a particular type of intelligence.

Lowenthal (1999) noted that the IC shouldn’t expect its analysts to serve as their own OSINT collectors and producers. He noted that there is not an end-to-end process for OSINT as there is in imagery, signals, espionage, etc. Extending from Lowenthal, training all source analysts to fully collect, process and exploit publicly available information would require the development of specialized skills, those often found in an intelligence collector, and would add to the ever-growing set of responsibilities placed on the IC analyst. In reality, this practice would clearly place the burden on each IC or DoD agency to emphasize the use of intelligence production and analytic time to be shifted to the production of OSINT, resulting in less time answering key intelligence questions.

Individual agency decisions to emphasize production of OSINT in lieu of performing long-established missions have not seemed to make great progress over the last decade.

Insisting that IC analysts learn how to produce relevant OSINT to meet both mission requirements, and to benefit the greater IC OSINT effort, may also not be in the long-term interests of IC agencies. A 2008 RAND Corporation paper titled "Assessing the Tradecraft of Intelligence Analysis" suggested that encouraging analysts to be "generalists" at the expense of subject matter expertise might be detrimental to the intelligence enterprise (Treverton & Gabbard, 2008, p. 7). This suggestion would argue that systematic requirements to make an all-source analyst act as both a curator of intelligence, and a producer, may limit their ability to develop a proper skill set necessary to be effective at both.

Established intelligence production methods within the IC also pose additional problems with distributed OSINT production responsibilities. Agencies engaged in all-source intelligence analysis, as well as agencies primarily engaged in the collection of secret intelligence, are unlikely to have production mechanisms for newly produced OSINT outside of their existing OSINT efforts. One potential pitfall of the lack of a production mechanism for OSINT would be that OSINT activities conducted by individual agencies that don't match existing production capabilities may actually impede in the production of OSINT. Not having a production outlet may mean that newly produced OSINT may not end up in the IC repositories, and instead end up as a citation or reference in finished intelligence, or worse only considered as background information. In either case, this newly "created" OSINT that is neither produced nor shared within the IC. Continuing, other IC entities may unnecessarily (and unknowingly) duplicate the same OSINT efforts in the production of OSINT. This process could occur time and time again across multiple agencies, which is hardly an efficient use of IC analysts time. In sum, distributed OSINT production places burdens on IC analysts outside of the OSC, and may be hurting OSINT's growth within the IC. This practice will likely continue to present long-term challenges to OSINT's future.

Changing analytical expectations. As the nature of the global threat has changed over the last 20 years, so has the focus of intelligence analysts within the IC. The preponderance of intelligence issues in today's 24/7 intelligence operations focus on answering intelligence requirements on short notice. Long-established missions for some IC analysts have been to conduct long-term analysis, largely free of the constant grind of current intelligence operations. Hart and Simon (2006, p.45), in "Thinking Straight and Talking Straight: Problems of Intelligence Analysis", noted this shift in intelligence analysis away from long-term research, towards more current reporting, by acknowledging that intelligence analysts are rewarded or incentivized by individual agencies based on the number of reports produced.

This continues to evolve within the IC, and the focus continues to shift to a more immediate requirement for producing intelligence today, largely due to the globalization of information, changing customer expectations, and the changing global threat environment where more information from more sources dictates more questions from the consumers of intelligence. This is especially true when customers largely have access to a growing amount of the same information available to IC analysts, and demand key insights from IC analysts that include intelligence from all-available sources (INSA, Expectations, 2012).

Best and Cummings (2008) outlined that one significant limitation for OSINT is the lack of subject matter expertise, or technical ability. Another is the potential analyst bias against OSINT; having to choose to answer immediate requirements, the IC analyst may choose to include information only collected through traditional clandestine methods. Best and Cummings noted other OSINT limitations that may be surprising to some, such as the “echo effect” (Best & Cummings, 2008, p. CRS-8) when the same information is reported by multiple information outlets and may inadvertently add to the credibility of the examined information by inferring that the information is supported by “multiple sources”. Others limitations found particularly notable for this examination are the increasing amounts of available data, the lack of tools to effectively find pertinent information relevant to intelligence requirements, and the “…overly rigid IC security practices…” (Best & Cummings, 2008, p. CRS-9).

Another important limitation for OSINT lies in the fact that all IC analysts may not have access to the Internet on their desktop to actually attempt the production of pertinent OSINT; those who do face increasing security requirements due to the changing security posture of the IC aimed to monitor and track employee Internet usage (Braun, 2014). Un-filtered searching across global sources that may prove valuable to OSINT also comes with risks, owing to growing cyber security threats. Finally, and as has been previously noted in Chapter 3, not all IC agency analysts have equal access to the tools and technologies based on the long-running, agency-centric technology acquisition practices. A lack of standardized tools and technologies within the IC to promote safe searching and the production of OSINT across the WWW mean that certain IC agencies enjoy the ability to produce important OSINT in support of their missions, while others lack the ability to do the same.

Technology and the IC

Although tools and technologies are mentioned as part of the solution for the emerging OSINT challenges, there are a wide variety of views of the utility of tools and technologies across IC personnel. Not only is there a lack of consensus among IC members on the definition of OSINT, there are also differences when it comes to assessing the inherent value of innovative tools and technologies developed to address IC requirements. A 2008 study by RAND indicated that "There is no consensus on the need or value of 'tools'". The RAND study indicated that the various IC analysts who participated in its survey had differing views on technologies and tools that ranged widely, from "…'the best thing since sliced bread' to 'evil and nefarious'." (Treverton & Gabbard, 2008, p. 19)

Decentralized OSINT technology acquisition & implementation. Realizing the wide-spread challenges to a centralized approach to OSINT, senior IC leaders have repeated the mantra that OSINT efforts can be centralized and supported (through the creation of the OSC, establishment of the ADDNI/OS, and the 2006 NOSE OSINT vision) but executed in a decentralized fashion. The process in this distributed OSINT model, designed whereby the members fulfill their own OSINT requirements to be shared with all in the IC, may present a limiting factor for the growth of IC-wide OSINT capabilities. While IC-wide improvements have emphasized information sharing and consolidation of existing OSINT resources from around the community and making them more available, developing institutional buy-in with IC agencies on the importance of future investments in OSINT seems to be wrought with challenges. Bean (2014) noted former OSC director Naquin’s thoughts on this issue in 2013:

> First, economic realities continue to limit individual agencies’ investments in Open Source, and with more austere budgets on the horizon, I would be surprised if Open Source-specific investments competed well. Second, if the prevailing school of thought is that the true value of open sources depends on how well they are integrated with more clandestinely acquired material, there might be less interest in building a distinct Open Source Enterprise. In an era of tight budgets, and despite the potential economies of scale, no one agency is going to be keen to resource an IC-wide Open Source program unless there is a greater commitment among individual agencies to build their own capabilities and contribute, in turn, to the enterprise. (Bean, 2014, pp. 44-45).

Historical approaches within the IC focused on meeting individual agency-centric technology requirements may also be thwarting long-term and major improvements for OSINT.

While IC agency-centric OSINT may be valuable to analysts across the IC, each agency makes decisions about what to purchase, or which program to fund, largely based on individual key interests and primary intelligence missions. Expecting IC-wide growth for OSINT while the preponderance of effort is focused on individual IC agency contributions, which are focused primarily on their own intelligence missions and requirements, may not produce the collective gains for OSINT as envisioned by the 2006 NOSE OSINT vision value of Gestalt – that the sum of the parts is greater than the whole (Jardines, 2006).

Current IC technology acquisition models favor private sector companies wishing to conduct business with or on behalf of the IC, including activities related to OSINT. The private sector largely depends on providing tailored tools and technologies designed to meet individual IC agency information technology requirements. These practices aim to acquire long-term government contracts, and private sector businesses aim to provide these tools and technologies, along with their support services, for extended periods of time. As noted previously, the acquisition and implementation of technological solutions to solve key issues are normally not based on a single acquisition of a tool or technology. Information technologies require maintenance, training, and long-term commitments to maintain, provide support, continually update and upgrade as new functions are developed, and so on. Private sector business models for technology acquisition are leveraged in favor of the current agency-centric solutions, relying on large contracts for the individual IC agencies that have larger fiscal resources. The private sector counts on the currently fragmented and decentralized technological marketplace that is today's IC. Attempts to change this practice in the future will likely meet resistance by the private sector unless the IC develops incentives to private sector technological innovators, or unless the IC builds a robust capability to develop its own capabilities to produce technological solutions in-house.

Unequal access to technologies. Decentralized IT technology acquisition practices have led to the unequal acquisition of tools and technologies amongst IC members. As noted in Chapter 3, there are large numbers of tools and technologies already implemented and in use within various agencies of the IC. Analysts who are provided with advanced OSINT tools and technologies have a distinct advantage over other IC analysts whose agencies do not share the same orientation, resources, and focus on OSINT. In regards to information technologies, all agencies are not created equal; some are created more equal than others. The unequal diffusion of OSINT tools and technologies scattered across the entities of the IC will continue to influence where OSINT advances occur in the future. The 2006 NOSE OSINT vision goal of creating a guild of OSINT experts within the IC was largely dependent on the additional training of future OSINT “champions”. This would require a standardization of available tools across the IC. The lack of ability to possess, have access to, or even use some available IC tools across the IC equally will likely hinder systemic OSINT efforts in the future.

Technologically challenged. As early as 1994, Nance wrote on the requirements for the necessary expansion of automated tools and systems to handle open source. He also argued for the needs in the expansion of information technology, stating “A clear, competitive advantage accrues to the organization or nation that fully and quickly embraces the new technology”. He recognized early on that the IC must become adaptive and more flexible, and that the military must address the system in which it acquires new systems so as to not fall behind in the generational-life cycles of new technologies (Nance, 1994).

While one could point to some technological breakthroughs for OSINT over the last 20 years, some may suggest that the current information technologies within the IC have fallen behind the technological curve. The WMD Commission (2005), speaking of the IC, found that “…it is behind the curve in applying cutting-edge technologies…” (Report to the President of the U.S., 2005, p. 5). INSA further concluded in a 2012 white paper that “The IC will be ineffective if it fails to assimilate these new and dynamic information technologies, capabilities, processes, and means of conveying knowledge to policy makers (INSA, Expectations, 2012, p. 15). In a recent response to a question on the plans to restructure IC information technologies, the DDNI Cardillo did not appear to relate much hope on the IC's capability to stay up to date in regards to technologies. He stated, in regard to the status of IC information technologies in 2012, that:

> Today, they [people] are inhibited by IT. I can go to a terminal to try to integrate across the IC, and be held back by email addresses, firewalls and classification levels. The IT is definitely holding us back today. It's much better than in 1983, but it still is holding us back. (Cardillo, 2012).

Treverton and Gabbard (2008) also suggests that two issues the IC faces in the development of technologies and tools are the lack of consensus on the value of tools, and the lack of the ability to determine analytical tool needs or requirements (Treverton, Gabbard, 2008, p. 19). Further, the authors noted that there are no real coordination mechanisms for the diffusion of technologies within the IC:

> Although there are multiple sponsors for technology, in the CIA and beyond it in the wider community, those sources or sponsors are mostly uncoordinated. Nor are there systematic mechanisms for transferring or inserting technology, both among and even within individual agencies. (Treverton & Gabbard, 2008, p. 19)

Their study reported that large discrepancies exist within IC member agencies in relation to the diffusion of technologies and found that some IC agencies report a dearth of tools, while others say they can't afford them. The lack of a coordinated feedback system within the IC to ensure that promising tools and technologies find a larger user-base will present challenges to realizing promising OSINT improvements across the IC.

Resistance to technology solutions. Despite the growing amounts of both classified and unclassified sources of information and a reliance on IT solutions to help make sense of the data, some within the IC still caution the reliance on technological solutions. Bean (2014) recounts the former director of the OSC cautions against the idea of a technological "fix" for OSINT. Naquin offers his reservations of technologies:

> 'Big data' is big in the USG [U.S. government], driven by the volume and variety of data now publicly available. Social media are a major driver, and the 'Arab Spring' served as a wake-up call. In general, though, the amount of data of potential intelligence value—and the digital incarnation of these data—has everyone talking about harnessing petabytes, exabytes, and so on. Fair enough, but I caution that we not overemphasize 'big data' as a technical challenge or believe that hiring an army of 'data scientists' will send us on our way to pressing F9 to predict the next social upheaval. While technology and greater statistical facility among those exploiting 'big data' might be necessary, they are far from sufficient.' (Bean, 2014, p. 49)

As covered by Bean (2014), Naquin would add that "Technology and statistical analysis should allow us to organize haystacks better, but I believe we will still depend on substantive—and Open Source—experts to derive insight from those haystacks, let alone find any needles" (Bean, 2014, p. 49). His observations do not address key issues that have yet to be resolved within the OSINT discussion, namely expanding the amount of open source experts outside of his former agency, the OSC. His thoughts also dismiss the reality that continued advances in world-wide information technology will introduce more and more information for the foreseeable future, and will pose challenges that will likely require even more advanced technological solutions.

External Influences

Too much information, too little time. The problems of too much information continue to grow, especially in regards to discussions concerning OSINT. Current efforts OSINT efforts within the IC have focused on the consolidation of available OSINT either on Intelink, through message distribution systems, or via the OSC Web site. However, these efforts continue to emphasize only the currently produced OSINT, and largely do not address the vast amount of open source information that may prove enough value to be collected and produced as OSINT.

But it's not just about too much OSINT. The amount of classified data seems to be growing as well. Time spent on one or the other shortchanges the full consideration of both, and choices have to be made. Time spent on the individual collection of intelligence information comes at the expense of the amount of time necessary to analyze the data, formulate hypothesis, and set out to prove or disprove an intelligence question. Of course there are other constraints on analyst's time, and as within any bureaucracy the size of the IC, administrative requirements can place numerous demands on an analyst's time. Some are necessary, as intelligence analysis is a tradecraft that must be learned, and the tradeoffs in some cases make logical sense. However, on the whole, time constraints on intelligence analyst's ability to adequately perform reasoned and sound intelligence analysis will continue to be a major limiting factor on the greater use of OSINT in finished intelligence production.

Sufficient analytical time is the enemy of today’s intelligence IC analyst. The sheer volume of information from both classified and unclassified sources continue to stress the already limited amount of time available for properly analyzing the information, or “connecting the dots”, when trying to address key intelligence requirements. The decentralized OSINT repositories that exist across multiple locations within IC information systems already limits the amount of time analysts can perform the separate research functions necessary to make complete and informed intelligence estimates and assessments. For example, recall that the 2006 NOSE OSINT vision aimed to compile all OSINT into a single information architecture. Currently, the OSC pushes out OSINT into a variety of internal information dissemination systems. The preponderance of the added benefits of OSC’s Web site remains physically separated from the majority of available intelligence information that reside on different, classified networks. IC analysts must still physically research the preponderance of available OSINT on unclassified networks to ensure they have access to the wide amount of provided OSINT, as well as to take advantage of the extra services that the OSC provides to its USG customers.

Robert Cardillo, then Deputy Director of DIA, former DDNI for Integration, and now the National Geospatial-Intelligence Agency (NGA) Director, spelled out the cumbersome processes involved in the gathering of data performed by today’s IC analysts:

> Data gathering is one challenge. Between open-source resources, message-handling systems, Intellipedia, Intelink, A-Space, LNI, and discrete dissemination mechanisms for sensitive intelligence, analysts could spend all day, for many

> days, seeking data. Once gathered, data can be cumbersome to array and analyze in ways that help make sense. (Cardillo, 2010, p.3)

This is alarming when once considers that these analytical limitations arise from the current state of available OSINT, and other intelligence that is already collected and produced. What is more startling is that the IC only harvests a portion of the deluge of available information available within the global information streams; imagine the stressors created by the collection of a vast majority of world-wide information pertinent to IC requirements. This is a daunting proposition that is almost unfathomable to tomorrow's intelligence analyst, and will likely remain an enduring challenge for OSINT.

There is also the notion that there are too many threats for the intelligence analyst to handle, and that the IC is adequately staffed with analysts to deal with the emerging global threats. While the IC has added a large number of intelligence analysts since 9/11 (Treverton, 2005), the IC requires a wide range of personnel to accomplish their mission including a wide variety of analysts, collectors, information technology, scientists, engineers, and support personnel, to name a few. The notion that IC is largely comprised of intelligence analysts overlooks the large number of personnel required to execute intelligence operations across the IC.

Russ Travers (1997), a former DIA employee, and later deputy director of the National Counterterrorism Center, foresaw coming changes in the IC pertaining to the amounts of information now available in today's information rich environment. The following is from the author's synopsis of the 1997 article looking ahead to the year 2001:

> The Community could still collect “facts” but analysts had long ago been overwhelmed by the volume of available information and were no longer able to distinguish consistently between significant facts and background noise. The quality of analysis had become increasingly suspect. And, as had been true of virtually all previous intelligence failures, collection was not the issue. The data were there, but we had failed to recognize fully their significance and put them in context. (Travers, 1997, p. 35)

Travers’ main point was that too much information in the future would cloud the IC analyst’s ability to discern important information from the multitude of available information, and that too much information would degrade the quality of analysis. A more recent article concerning information overload points to continued problems with information overload and its potential long term negative effects for the IC. Young (2013) stated that the U.S. IC collects a massive amount of information every day. He argued that this type of intelligence gathering only leads to information overload for both individuals within the IC, as well as for the overall system. As a result, the IC does not use this information effectively, and that the problem of too much information impairs the ability of the IC to effectively do its job (Young, 2013).

Conclusions

Dandar outlined many of these same constraints or system limitations nearly twenty years ago. He made assertions that IC analysts do not have the time, or training to continually exhaust information on multiple targets of interest based on the vast amount of information sources available in 1997. He also argued that the distribution of intelligence analysts across the IC in the various agencies also presents limitations for the greater incorporation of OSINT. He lamented that intelligence analysts work within a "…fragmented systems environment with uneven connectivity to resources and widely varying practices, methods and tools for managing, accessing and exploiting information" (Dandar, 1997, para. 5). Nearly 20 years later, his observations still hold true and the IC continues to face these and similar issues when trying to produce gains for OSINT, especially when examining the limitations and institutional practices that continue to thwart tangible gains through the effective acquisition and implementation of tools and technologies.

While there have been OSINT successes noted thus far, this chapter outlined many limitations and constraints that have held OSINT back from realizing major system-wide improvements that specialized tools and technologies may offer in helping the IC make more effective use of the deluge of OSINT. The IC continues to make marginal progress in addressing recommended OSINT reforms and improvements that many advocates have envisioned for years, however these efforts fall short of an imminent paradigm shift. The lack of major progress for OSINT within the IC becomes clear in a 2012 INSA Rebalance Task Force White paper, "Expectations of Intelligence in the Information Age". This task force, comprised of many former Senior IC and USG officials, including a former DNI, highlighted that the IC will need to continue to expand its reliance on open sources of information, to a much greater degree than has been accomplished to date to accomplish their (IC) mission to fully serve policy makers (INSA, Expectations, 2012, p. 5).

CHAPTER 5

CONCLUSIONS

> “The Intelligence Community (IC) must fundamentally rethink its approach to, and the value of, open-source intelligence in response to dramatic changes in the global information environment”. (Central Intelligence Agency, 2001, Are You Ready?)

OSINT’s Future

OSINT has always played an important role in intelligence operations throughout the existence of the IC. Its importance has been noted since the very beginning of the IC in 1947. Through all of the scrutiny and recommendations of past intelligence reform commissions, both government-sponsored and those conducted and recommendations from the private sector, a clear and consistent trend has been that the IC should rely more on the use of publicly available information coupled with intelligence collected from clandestine methods.

Past efforts to improve OSINT within the IC have experienced many challenges. Even though long established as important, OSINT still finds itself as an outsider amongst intelligence disciplines despite the fact that the IC has made tremendous strides in providing new, and potentially invaluable sources of intelligence from the growing amounts of publicly available information. OSINT reached its peak of popularity early in the existence of the tenure of the first and second DNI. Their efforts to promote OSINT as a viable intelligence source will be evident for some time to come. However, as an institution, OSINT will continue to face obstacles in the future that may inhibit its full potential as outlined in the 2006 NOSE OSINT vision. This chapter relates what has happened to OSINT since the mid 2000' efforts at painting OSINT as a topic that warranted increased attention within the IC.

Lost Momentum?

OSINT advocates argued for years that OSINT should be the "source of first resort" and itself could answer upwards of 80% of intelligence questions. The first goal outlined in the 2006 NOSE OSINT vision adopted the position that OSINT should be the source of first resort. It appears likely that long-time OSINT advocate expectations and proclamations on the value and role of OSINT for the IC heavily influenced the early composition of the goals set forth by the NOSE. As was outlined in Chapter 4, the IC is a complex system, a consortium of agencies with shared missions, but with differing views on the inherent value of OSINT, a lack of consensus on its place, or even its definition. Cultural limitations, along with a host of other issues, have thwarted past efforts to move OSINT forward as envisioned in the 2006 NOSE OSINT vision. In particular, the ideas that OSINT, by itself, could replace 80% of traditional intelligence have failed to materialize tangible results toward this end.

The two DNI sponsored Open Source conferences were possibly the most "open" intelligence conferences ever to be held by the IC. These conferences served as a showcase for OSINT as an idea whose time had finally come. Although the conferences may have served a purpose, Bean (2014) noted former OSC director Naquin's comments on the lack of momentum for OSINT generated after the two DNI sponsored Open Source conferences by lamenting that, in reference to OSINT's place within the IC "…that the conferences did little to fundamentally revise underlying institutional logics and commitments" (Bean, 2014, p. 46). Based on available information from the DNI's

Web site, OSINT was still emphasized at other intelligence conferences in both 2009 and 2010. However, OSINT was hardly mentioned and noticeably absent from speeches made by the DNI and other senior ODNI officials from 2010 forward (DNI's Web site, 2014). In the most recent national intelligence strategy published by the DNI, the 2013 National Intelligence Strategy (U.S. National Intelligence, 2013), OSINT was not highlighted as a separate or discrete issue as it had in the past. It appears that OSINT, as a separate and distinct IC initiative, had lost its momentum.

One could note that OSINT seems to have lost momentum in recent years as the IC reform efforts focused on other more pressing, systematic issues, namely IT practices and the ever increasing intelligence demands of the changing global threat environment. While OSINT efforts still exist within the IC and will naturally continue to evolve and improve over time, more urgent matters may have subsumed the DNI's attention regarding overall IC issues.

Reform Expectations Not Achieved

The U.S. Congress made it clear in the post 9/11 days that the IC should rely on, and use more OSINT in the conduct of its business. Past efforts at building OSINT capabilities within the IC that worked toward the goals envisioned in the 2006 NOSE OSINT vision are highlighted throughout this thesis. Did the establishment of OSINT advocates and champions, the ADDNI/OS, the NOSE, the OSC, along with a multitude of implemented technologies within the IC produce the results envisioned by the reform efforts and mandated by the IRPTA? What impacts did these efforts have on the improved used of OSINT within the IC? Is real reform for OSINT possible within the IC?

There are other explanations necessary to explore. Two former senior IC officials analyzed past outcomes of IC reform recommendations over the last sixty years. Dr. Michael Warner of the Office of the DDCI, and Dr. J. Kenneth McDonald, former CIA Chief Historian, suggest that intelligence reform efforts since 1947 have produced only "limited and fragmentary change" (Warner & McDonald, 2005). Their report also noted that there were factors surrounding the reform efforts that "predicted" success and ranged from the quality of the reports, their sponsor, their timing and whether they occurred during a time of conflict, and so on. System limitations and constraints outlined in Chapter 4, especially in regard to OSINT, may also have relevance when re-examining their key findings. A casual observer to the OSINT reform recommendations, IC initiatives, and public discourse over the last several decades could argue that the U.S. has been in a "conflict" period over the last decade, during the height of OSINT's popularity amongst government leaders which ultimately led to the establishment of a formal OSINT vision. OSINT reform efforts over the last ten years, the authors would argue, should have had a positive influence on making real progress toward these reform recommendations. As the U.S. winds down a long-period of conflict, it remains to be seen if OSINT can achieve the kinds of success "predicted" by this examination of previous reform recommendations.

OSINT Changed Direction

The 2006 NOSE OSINT vision, as directed by the first DNI, was later revised and subsumed by information sharing and integration initiatives of the IC. In the IC published National Open Source Strategic Action Plan (NOSSAP) from 2009, the chief author of the plan, former OSC Director Douglas Naquin, offered his thoughts on the direction of OSINT within the IC "…The National Open Source Committee (NOSC) is now narrowing the aperture to focus on those areas that will maximize benefits to the larger open source enterprise while facilitating the work of those who are developing their open source capabilities" (National Open Source Committee [NOSC], 2009, p. 2). This view diverged somewhat from the original 2006 NOSE OSINT vision, where OSINT was treated as a commodity worthy of discrete attention to be used as the source of first resort in intelligence analysis. This plan largely outlined the importance of the integration of OSINT with all other intelligence disciplines to benefit the greater IC enterprise. The NOSSAP plan stated that "…the 'Open Source Enterprise' must focus on integration – both among the capabilities that exist within the open source community and between the collective open source and the broader intelligence enterprises." This revised vision for OSINT emphasized integration of OSINT within all sources of intelligence, and left out the idea of using OSINT as the source of first resort. This vision also focused on ensuring that already produced OSINT was made readily available across the IC on all networks. The NOSSAP plan reiterated previous falls for the creation of more OSINT experts and training curricula throughout the national security community. This plan also aimed to develop capabilities within IC entities to provide unique OSINT production or services (continued distributed production of OSINT), the use of partnerships from the commercial sector, academia and foreign entities, and to bring OSCAR-MS to its initial operating capability, to list a few. On technologies, the plan specifically mentioned a goal to grow foreign language processing capacity using language processing technology. Gone were some of the ideas and OSINT advocates of the past; now OSINT activities would be directed by the DNI with the assistance of the

Open Source Board of Governors. This new OSINT plan largely left out specific plans to introduce or develop new tools or technologies to help analysts deal with the growing amounts of information available in the public domain, much of which has potential as to become OSINT (NOSC, 2009).

It's not that IC seniors haven't thought about the long term importance of OSINT. The DNI publication *Vision 2015*, published in 2008, offered some insight on the direction of the IC and the future importance of integrating all forms of intelligence in the future 2015 IC. Emphasizing the importance of OSINT, *Vision 2015* offered that "No aspect of collection requires greater consideration, or holds more promise, than open source information; transformation of our approach to open sources is critical to the future success of Adaptive Collection" (2008, p. 12). *Vision 2015* also made some interesting claims that are, now one year from the stated 2015 goal, unsubstantiated in that "Information overload will be averted through sophisticated data preparation and tools" (2008, p. 13). One could argue that the IC has barely begun to get a handle on issues surrounding information overload, including all forms of intelligence and especially OSINT. Despite notable achievements in technologies thus far along with forthcoming developments in tools and technologies, the IC will face challenges associated with information overload for decades to come.

Another important aspect listed in the DNI *Vision 2015* (2008) was the future direction of technology within the IC. The plan called for building a Net-Centric Information Enterprise based on a common information architecture, based on sharing, to turn the "deluge of data" into predictive, actionable intelligence. This vision was to be accomplished by changing how data is separated by classification and by discipline into a:

> …unified architecture designed around a common ‘cloud’ containing our information. This information infrastructure will allow authorized end-users to discover, access, and exploit data through a range of services, from federated query to integrated analytic tool suites. (*Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*, 2008, p. 14)

Vision 2015 also related a familiar story on the importance of technology innovations, and the need for the IC to adopt private sector solutions by changing acquisition and procurement policies, with an emphasis on adaption, speed, and agility (*Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*, 2008, pp. 16-17). To this end, the DNI began initiatives several years ago that are moving some technology acquisition practices toward a more institutionalized, IC wide process. This has developed into a new IC-wide common information architecture called the IC ITE.

The move towards IC ITE. The DNI approved a strategy created by the IC CIO in 2012 to move the IC away "…from the historically agency-centric IT approach to a new model – that of a common architecture and operations as an IC-wide enterprise", is referred to as IC ITE (IC ITE, Doing in Common What is Commonly Done, 2012, p. 1). The primary objectives for the new common architecture state:

> …that the majority of IC Missions will benefit from improved agility, scalability, and security while realizing lower operating costs through the shared use of commercially developed IT and computing advances such as cloud technologies,

> virtualization, thin-client desktops, bid data analytics, application stores, and improved security. (IC ITE, 2012, p. 2)

Miller (2013) captured the IC CIO, Tarasiuk, comments in 2013 that the IC had established the "…first substantiation of the IC cloud with storage, data hosting and virtual hosting capabilities." Tarasiuk also spoke on the creation of an application mall that went online, with a number of apps in the mall that "folks across the community could use". Tarasiuk also noted that the single desktop tool was only currently available to two IC agencies, while "…the cloud infrastructure and the apps store are available to all IC employees with a top secret, sensitive compartmented information (TS-SCI) clearance" (Miller, 2013).

While the long term OSINT benefits stemming from the implementation of the cloud are yet to be realized, INSA noted in a 2012 white paper "Cloud Computing: Risks, Benefits, and Mission Enhancement for the Intelligence Community", that cloud computing can be a key mission enabler, helping to deal with issues surrounding big data. INSA noted that "Cloud solutions can now be used to work on all of the data, all of the time" (INSA, "Cloud Computing", 2012, p. 7). However, DNI Clapper noted in 2011 that Cloud computing does not solve all mission or technology challenges, and that establishing a Cloud computing environment "…requires careful consideration and the development of a business case with total cycle costs included" (INSA, "Cloud Computing", 2012, p. 7).

Ben Iannotta (2013), Founding Editor of Deep Dive Intelligence and now editor-in-chief of Aerospace America, noted in 2014 that continuing reductions in the IC's budget, the DNI's fiscal planning authorities may achieve some efficiency through the newly implemented IC-wide plan for technology acquisition. “The Intelligence Community Information Technology Initiative is supposed to reduce the community’s annual IT pending by 20 percent by 2018” the article stated. However, not all the savings would occur at once. “The savings would come gradually, a CIA official said, because the new community-wide operating system would be run in parallel with existing networks until managers gained enough confidence to unplug the old ones” (Iannotta, 2013). This article also points to the future consolidation of technologies across the IC. The article would also offer that:

> “If the plan works, agencies would no longer operate their own unique operating systems for top secret work. That change plus a shift toward cloud computing and adoption of apps are supposed to offset reductions to the $80 billion annual intelligence budget.” (Iannotta, 2013)

It appears that future IC budgets are betting on the reduction of spending on technology acquisition, as the current IC draft budget has proposed a 5% reduction in spending (Fryer-Biggs, 2014).

The long-term prognosis for OSINT within the overall IC ITE initiatives and the move to cloud computing remains unknown. Resetting the IC’s information architecture from a historical agency-centric model to a common IC-wide information architecture may provide opportunities for the IC to make systematic improvements that will benefit OSINT over the long run. The resulting technology acquisition practices dictated by the new information architecture, along with the resulting acquisition of new tools and technologies aimed to allow analysts to examine big data hosted in the new cloud, will continue to unfold over many years. As this data is aggregated, the IC has an opportunity to develop system-wide tools and technologies to help analysts mitigate information overload. The effects on generating tangible, and positive results on the acquisition and production of OSINT from the vast amount of publicly available information will be worthy of additional study as the effects of these initiatives ripple through the IC in the coming years.

OSINT Success Stories

OSINT's prominence has certainly grown over the last several decades, and continues to make positive inroads within the IC. The rise in the amount of OSINT that is produced continues to make positive impacts on intelligence analysis within the IC. OSINT's prominence as an intelligence source, or discipline, also continues to contribute to the problems of information overload within the IC. Chapter 3 showed many examples of the kinds of technologies implemented by the IC with the goal of finding solutions to improve the ways in which OSINT is produced, as well as used by IC analysts. Some of these technological solutions hold promise for the future. Other technologies already implemented and previously discussed will likely be discarded and replaced in the future by newer technological innovations. More importantly, the IC will continue its efforts to find and implement technologies that will help it manage OSINT, as well as the other intelligence disciplines, as they find favor within the private sector, or are fully developed and implemented by tech-savvy IT personnel. The following sections highlight some of the tools or technological innovations that achieved some of the goals outlined in the 2006 NOSE OSINT vision and improved overall OSINT practices, and tools and technologies to watch in the future. Although this thesis examined tools and technologies aimed to help the IC with various OSINT issues, solutions may not be as easy as finding the “technological silver bullet”. Private sector initiatives still face obstacles in getting at the multitude of available data and making sense of it.

The development of OSCAR-MS can be viewed as an important milestone for OSINT. The combination of existing open source collection requirements systems into a single system for use by IC analysts provided added functionality and process improvements for navigating OSINT within the IC. The long-term impact of OSCAR-MS is unknown, as information is scarce post-implementation. If OSCAR-MS ultimately succeeds through widespread diffusion and acceptance by IC collection managers and analysts, it could provide real benefits to IC users by allowing discovery of known OSINT, revealing where OSINT requirements have been met, and show intelligence requirements that have not yet been answered. This could reduce the amount of duplication in the production of OSINT throughout the IC by allowing analysts to see which requirements have yet to be answered by OSINT. This could also prove useful in determining successes in OSINT in order to bolster arguments on its value, and show OSINT’s potential role in reserving scarce classified resources to be used only for truly difficult information to obtain.

As described in Chapter 3, the IC as a whole have developed some and has invested in a variety of tools and technologies aimed to allow IC analysts to examine large sets of both structured and unstructured data. There are notable examples of data mining, text mining, link analysis, visualization, language translators, and other tools aimed at making sense of the vast amount of available data. The OSC continues to produce the majority of OSINT for the IC while at the same time providing an on-line presence that provides a multitude of database subscription services that can be widely accessed by authorized government and IC users.

How these tools and technologies continue to be acquired, implemented, accepted by users, and utilized by IC agencies to solve important issues and opportunities for OSINT remains to be seen. With the 2006 NOSE OSINT vision no longer the guiding vision, the prognosis on the impacts that technologies will have on improving OSINT within the IC remain unknowable. With the NOSCCAP OSINT goals outlined in 2009 in play, the principle of the development of open source centers of excellence may continue to emphasize an unequal distribution of OSINT tools and technologies across the IC.

Developments to Watch

Future developments in tools and technologies being researched, developed, or funded by In-Q-Tel and IARPA, and private sector companies appear to be in the early stages of developing the ability to begin to tackle issues surrounding big data, or information overload. Advances in data mining, and other referenced advanced technologies like artificial intelligence may be key to moving some of the requirements from human decisions to a more automated approach to predicting future OSINT from the mountains of available data. Although humans will always play a role in analysis, more advanced technologies may provide key "reasoning" for future OSINT production.

Specific to OSINT, the IC's CIO Tarasiuk (2009) mentioned in 2009 that the OSC in collaboration with the IC was working:

> …to develop an integrated community OpenSource [sic] architecture where the vision is that anyone working on OpenSource [sic] anywhere in the DOD and intell [sic] community would have access to a common set of tools and a common

> set of data to help them do their job. It would be network agnostic and platform agnostic. (Tarasiuk, Remarks at the 2009 GEOINT Symposium, 2009).

Although the results of these efforts remain unclear, access to a majority of the available OSINT and access to a common set of tools and technologies would be an important step forward in providing IC analysts the ability to improve the conduct of OSINT in the IC.

In 2012, a Defense Systems report indicated that the DIA and the NGA were developing a common desktop, with DIA in the lead. The initial focus is on providing common tools, mobility, and access to data for IC analysts. It also confirmed movement toward the establishment of an IC cloud, with the ability of each agency to develop applications that would provide access to their intelligence products and databases (Rosenberg, 2012). Although OSINT was not specifically mentioned in this article, one can certainly imagine the proposed applications that may improve the access to all OSINT available within the IC from a single location. Will the newly established Cloud finally provide OSINT with the ability to come close to satisfy the original 2006 goal of being the source of first resort?

DARPA (Harris, 2014) is reportedly working on a project to watch regarding its potential application to solve some OSINT challenges. The project called Deep Exploration and Filtering of Text (DEFT), aims to provide the ability to "…analyze textual data at a scale beyond what humans could do by themselves." DEFT harnesses natural-language processing technology to more efficiently process text-based information to enable to understand connections that might not be apparent to humans. If this effort proves successful, DARPA projects that "…DEFT will allow analysts to move from limited, linear processing of huge sets of data to a nuanced, strategic exploration of available information" ("DEFT" search, www.darpa.mil, 2014). Technological innovations such as DEFT, and others, will be essential looking forward to develop the types of automation that may be critical to improving the ways in which potential OSINT is collected, processed, and analyzed.

Social media. The IC's emphasis on social media to monitor world-wide trends and sentiments appear to be well entrenched and will likely remain an emphasis for some time to come. Bean (2014) recounted former OSC director Naquin's opinions on the immediate future for OSINT "I believe Open Source is increasingly accepted as essential to the intelligence process, and social media and 'big data' are the latest drivers in raising its profile" (Bean, 2014, p. 49). INSA noted that the exploitation of social media now provides sentiment analysis and indications and warning information that a few decades ago would have been considered secret information (INSA, Expectations, 2012, p. 13). Based on these insights, along with the DNI's support for social media outlined in Chapter 3, social media analysis will likely remain a prime source for OSINT by the future IC.

Foreign language translations. Another important technology that needs further refinement are public and IC developed automated foreign language translations tools that provide translations from both written text or from audio files. The long-term noted deficiency of linguists within the IC and the military will likely never catch up the increasing demand for this kind of support to OSINT, and to other intelligence producers. An increased diffusion of tools and technologies to IC analysts which provide automated translations of foreign sourced data may prove important to exploiting the vast amount of the potential OSINT within global information stores. However, Wyatt Kash (2010), Editor-at-Large with *Federal Computer Week*, captured the CIA Chief Technology Officer Gus Hunt's thoughts on the state of machine translation capabilities in the future. Hunt commented that "There hasn't been a major breakthrough in this space for a long time." Hunt later added:

> I am going to be honest: I thought machine translation and…voice recognition were technologies that would have been well solved by today. I thought that many years ago, [and] these are two areas where either I was overly optimistic or way off base. But today, I don't see a good, high-performance, high-accuracy solution emerging anytime in the next five years. (Kash, 2010)

What's Left Behind?

Expanded reliance on OSINT within the current integration initiatives still focus on particular aspects of OSINT, namely social media, and sentiment analysis, and the long established sources. These only represent only a small portion, albeit a potentially important part, of the potentially available OSINT sources. Further examination of the these types of OSINT and their abilities to answer intelligence questions will be necessary to continue to identify areas of OSINF that is not being collected and processed as OSINT. What are the missed opportunities in OSINT that will continue to accumulate? Will the IC ever get their hands around the breadth and depth of the available global information to fully inform U.S. policy makers? What is being left behind, uncollected, unconnected within big data? What is not being collected and harvested to become OSINT? The IC has certainly not exhausted all potential sources of data, and it would be premature to stop exploring new sources.

Future, Meet the Past

The IC is a large bureaucracy that is risk averse and is used to making measured, incremental improvements. This means that the IC is likely to continue to make small, calculated changes to improve its intelligence, regardless of the source of the information. Rolington suggests that no matter how important the raw intelligence may be (in this case, think of OSINT), that the cultural context within how it has been produced is also influential (Rolington, 2007, p.743). He recounts two organizational principles that share the view that "…organizational plans for the future are inherently linked with already evolved patterns from the past" (Rolington, 2007, p. 742). The mid-2000 approaches to OSINT as the source of first resort may well have been too far outside accepted norms for the IC. The current IC direction towards IC ITE has subsumed future OSINT efforts underneath information sharing and integration initiatives and continues to emphasize a distributed approach to building more OSINT experts and defined OSINT centers of excellence. Rolington (2007) also notes that organizations are the creatures of their times – usually designed in reaction to a given set of historical circumstances. In this case, U.S. national security ties the IC together. An organization's culture reflects this atmosphere and, more important, their methodologies, processes and outputs also reflect the reasons for their initial creation. The IC exists to find answers to national security requirements, whether or not an adversary wants to keep said information that answers these questions a secret. Referring back to Lanheman, maybe the IC with its secret mission, environment, and orientation toward secrecy will prevent OSINT from becoming what it was once envisioned.

To the credit of the first DNI, the IC did design a vision for OSINT, and desired to build a guild of champions and OSINT advocates through the early OSINT initiatives.

The goals and vision for OSINT seemed destined to finally realize real gains and finally earn OSINT respect within the IC. In 2014, however neither the ADDNI/OS, the chief IC OSINT champion, nor the ICD 301 still exist in 2014. Bean (2014) reported former OSC Director Naquin's statement that the IC "champion" for OSINT has found its way (back) to the CIA, with the Director of the CIA, where it was found when FBIS was part of the CIA. Is this the progress envisioned for OSINT in 2006?

With the IC focus on intelligence integration, all past OSINT efforts were not made in vain. OSINT is still emphasized as playing an important role in future intelligence production (INSA, Expectations, 2012). Future technology-based solutions to big data problems may also prove more successful within the IC once the issues of information integration occur within the cloud. The IC move to cloud computing may also improve the ways in which data are consolidated, and future tools, technologies, and applications that are in development may still hold promise to help OSINT rise to its much recommended, greater role within the IC.

While integration efforts and developments in the IC's move to cloud computing continue to be developed and rolled out, interim steps should be considered to determine current best practices, and the best tools and technologies to consider for more widespread implementation across the IC. INSA noted a key finding about the IC's move toward cloud computing, arguing that "Lessons learned from the IT industry, the private sector, and academia must inform IC decision making. Sharing lessons learned is essential to reducing risk"(INSA, Cloud Computing, 2012, p. 1).

The IC can ill afford more years of not getting a handle on the deluge of potentially valuable information that can be acquired, processed, and exploited into invaluable OSINT. While these initiatives sound promising on their merits, it will be interesting to measure these new efforts against the IC-wide challenges and limitations outlined in Chapter 4 in the coming years to see if the IC can finally realize new technological gains for OSINT. This examination outlined many challenges and limitations for OSINT; some were new revelations, some repeated, familiar arguments that may have kept OSINT from achieving its full potential within the IC. In any case, if the past is any predictor of the future, systematic issues surrounding OSINT may continue to face familiar, as well as newly identified challenges, in the future.

Long Term OSINT Challenges

Moving forward, the IC will continue to face many challenges in its quest to improve the production and use of OSINT in intelligence operations. Chapter 4 highlighted many system-wide challenges and limitations that have stunted attempts thus far to realize improvements in OSINT through the use of information technologies. System-wide challenges will continue to stress the IC for the foreseeable future. The following sections outline some pressing issues that the IC will need to overcome for OSINT to see lasting, and tangible improvements.

Information overload continues while big data grows. The opportunities and challenges of the information revolution, or big data, have made an indelible mark on the IC. Big data is said to be both a blessing and a curse. One thing that appears certain is that it is unlikely that the amount of publicly available information will decrease over time. The IC will continue to spend precious resources and capital on developing solutions to ensure the efficient use of this information to conduct its business. If the IC doesn’t soon make substantive improvements in its ability to harness this information, to make sense of it and use it to its advantage, will it continue to maintain the competitive advantage in information technologies in the world? Will it ever get ahead of the information technology cycle, as Nance suggested as necessary or be relegated to playing catch up (Nance, 1994, p. 9)? Will the next major intelligence failure be similar to the past, in that key information was available within existing intelligence data but not discovered in time to prevent an intelligence failure from occurring? Which technologies have not properly been implemented that could have “connected the dots” from within the available data? Will the next intelligence failure be a result of collecting too much information coupled with the inability to effectively make sense of the data? These issues continue to present real challenges to the IC of the future.

Fiscal realities. History shows that the periods following the conclusion of conflicts usually mandate downsizing and budget reductions throughout the IC. After the fall of the Soviet Union, the U.S. IC was subject to a congressionally mandated downsizing, estimated by the former DDCI John E. McLaughlin speaking at the Conference on CIA's Analysis of the Soviet Union, 1947-1991, at Princeton University, at 22% (McLaughlin, 2001). As the war winds down in Afghanistan, and the U.S. draws down its forces, war-time operational intelligence requirements will lessen and it is likely that Congress will once again demand a peace divided from the military and intelligence components of the government. Although there are situations where OSINT will receive dedicated streams of funding, many developing and innovative tools and technologies for OSINT will continue to compete with traditional intelligence programs (secret) from scarce funding sources.

Technological innovations. One thing is certain. As long as big data provides opportunities for new knowledge for the IC, and as the expectations for the IC in the 21st century continue to evolve, there will be a need for the IC to harvest all available information, regardless of source, to provide a more complete intelligence answer to the consumers of intelligence. Private sector companies will continue to stay in-tune with issues of the day, and continue to develop new and tailored technologies for their own use in business and competitive intelligence.

The future IC, if it requires technological solutions to be shared amongst its agencies, will require business transactions to change from the existing business model of tailored, agency-centric solutions to solutions that have IC-wide application. One can only wonder what new products and services will be developed once the IC moves to a common information architecture pushing all available intelligence to the cloud (including OSINT), along with efficiencies in processes, along with unfettered access to all available OSINT, as envisioned in the new enterprise IT solution, IC ITE. Only time will tell.

Risk aversion. Chapter 4 identified IC limitations, or system constraints that may hold-back, or have prevented real OSINT reforms thus far. With much of the new public information available on the Internet, it was even noted that not all IC analysts have access to the Internet at their desktop due to security concerns. IC analysts face a growing number of on-line threats and adversary instituted cyber-related activities. To this end, the very process of conducting searches on the Internet for OSINF to be collected and produced as OSINT, collecting new potential OSINT necessary to meet mission requirements, may actually expose IC analyst’s to cyber threats from malicious actors. Will the IC ever fully realize the benefits that the individual analysts can make in the production of OSINT, or will the IC continue to solely rely on the contributions of the OSC as the main producer of OSINT?

Failure to define OSINT. Future OSINT initiatives will likely face similar issues of the past where institutional bias and the lack of a common definition of OSINT have plagued previous OSINT initiatives. Bean reported Naquin's thoughts on whether OSINT has successfully been institutionalized within the IC, noting that ‘‘One could certainly argue that the creation of a DNI center represents the institutionalization of open source in the IC, but as of February 2012, most IC institutions had not yet altered their thinking on open sources in a programmatic sense, e.g., as an area worthy of discrete attention’’ (Bean, 2014, p. 45). Naquin also cautioned that while OSINT is increasing accepted as essential to the intelligence process, he noted that until the IC and national security community accepts OSINT as a discipline versus a commodity, that OSINT efforts will be fragmented and assessing how well the IC is doing at OSINT will be difficult (Bean, 2014, p. 49).

Private sector initiatives and challenges. While the IC has struggled to achieve the goals of OSINT, the private sector continues to gather and analyze as much data as possible to predict consumer behavior, develop marketing market data, improve operations, provide information for product development, and improve human resources. The *Wall Street Journal* published an article in March 2013 suggesting that as organizations continue to collect more and more data, the "tab keeps growing, too", that is companies are spending more and more to try and make sense of the data (Rosenbush & Totty, 2013). Whether the IC can match this practice of increased spending on technological initiatives to aid in the creation of more valuable OSINT remains a question that needs to be answered in the coming years if real OSINT reformed is to be achieved.

However good private sector initiatives may appear, one private sector effort aimed at getting a handle on big data did not prove as successful as information giant Google would like. David Lazer (2014), a joint professor in political science and computer science at Northeastern University, wrote on the failure of Google flu trends on the Web site *MIT Technology Review (*2014). Lazer proclaimed that Google flu trends has long been touted as the “go-to example for anyone asserting the revolutionary potential of big data” (Lazer, 2014). He also noted that Google flu trends had drifted away from accurately predicting flu outbreak trends since 2008. If Google experienced issues with trend analysis, what does that say to the future of the IC’s emphasis on Social Media? While initiatives and technological innovations in the private sector may hold real promise for future IC OSINT reform efforts, the IC should be realistic in its future approach in the development of tools and technologies to deal with big data, and aim to develop or acquire the right tool for the right job, as well as determine the desired outcomes, and plan resources and efforts for the long-term to address specific issues instead of only focusing on a short-term fix to today’s issues.

The DNI will continue to force discussions and initiatives focused on OSINT, as well as direct the creation or establishment of certain capabilities within the IC, including the potential creation of additional “centers of OSINT excellence” within the IC to augment the long-time and valuable contributions of the OSC. These efforts will likely face similar limitations such as institutional bias, along with others outlined in Chapter 4, especially without IC-wide OSINT advocates. The IC will make changes, although at a slow pace, with future directions firmly rooted in the past. The initiatives that stem from IC ITE will likely force the issue in some areas. INSA (2012) repeated many past calls for OSINT reforms and made an interesting proposal to establish OSINT as a new intelligence discipline, and to guide how OSINT is conducted within the IC in the future (INSA, Expectations, 2012). Unless the IC collectively is able to overcome a bias toward OSINT, or even more important, establish a common definition of OSINT within the IC, these sentiments will likely persist within the coming years, as agency missions continue to become more complex in answering the ever changing intelligence requirements for their customers.

Will OSINT re-emerge? OSINT has been a favorite topic within the IC over the past six decades. It is problematic that its value and worthiness as an issue worthy of discrete attention continues to appear almost cyclically within the literature. The CIA published an unclassified project report regarding its future view of OSINT in 2001 (Are You Ready?, 2001). This effort projected that the IC must rethink its OSINT approach, and the way it values OSINT, to maintain the ability to respond to changes in the globalization of information (p. i). Numerous commissions and intelligence community efforts since 2001 have focused on improving OSINT through a variety of programs, initiatives, visions, and practices. INSA (2012) reiterated long-time recommendations for OSINT in 2012, that “The heightened expectations of decision makers for timely strategic warning and current intelligence can be addressed in significant ways by the IC through “open sourcing” of information”. INSA also notes that in the future the IC will need to expand its use of OSINT, while continuing to perform traditional intelligence missions, in order to fully serve IC consumers (INSA, Expectations, 2012, p. 1). That INSA has started to espouse the same recommendations made over the last 60 years reveals that OSINT, since its peak of popularity just a few short years ago, has lost momentum within the IC. If the past is any indicator of the future, OSINT will likely re-emerge as a discrete topic, worthy of attention. When is a different question altogether!

Will a more technologically savvy workforce drive changes in OSINT? The growth of the technology over the last several decades, along with the new influx of younger intelligence analysts, does provide hope that OSINT challenges can be overcome. Treverton reported in 2005 that a large percentage of new intelligence analysts in the IC since 2001 have less than 10 years experience (Treverton, 2005). Incoming intelligence analysts, borrowing from their own exposure and experiences with technology within their daily lives, as well as the deluge of information available in the public sphere, will continue to provide the push for a greater use of OSINT and will likely push for and embrace new technological innovations that will be necessary to fully realize the benefits of OSINT within the IC. If the IC continues to lag behind the private sector in technological solutions to long-running issues such as big data, these analysts may become frustrated. Treverton cautioned the IC in 2005 to ensure wise and efficient use of technologies to solve IC challenges, along with ensuring that it keep up with the younger, more technologically savvy intelligence analysts:

> Finally, the next generation of analysts has much more experience with and is much more comfortable than its seniors with information technologies, networked environments, and parallel processing of large amounts of information. These young people access data, share hypotheses, create “problem-centric” networks,

> and communicate in parallel with their friends in ways that will shape how analysis will be done in the future. Gilman Louie, former president of In-QTel, describes a wide range of technologies and concepts for using them that the modern student uses for purposes of learning, socialization, and accessing and storing data that are a far cry from today's intelligence architecture. The Community will not attract, or will soon lose, these young people if it does not accommodate to how they think and learn. (Treverton, 2005, p. 31)

The idea that younger analysts will drive necessary technological changes to positively impact OSINT deserves further attention, especially given the IC's slow progress on OSINT thus far.

Why Haven't Technologies Fixed OSINT?

This thesis set out to see why technologies haven't fixed OSINT within the IC. Chapter 4 showed how many IC structural and cultural constraints have limited the abilities of tools and technologies to dramatically improve OSINT. Chapter 3 related that to date, the IC has made some progress in attempts to employ new (and old) technological solutions for OSINT. A large portion of the success of OSINT has been noted numerous times in the establishment of the OSC along with its Web site at www.opensource.gov. Select IC agencies have made significant investment in building OSINT capabilities and have implemented innovative tools and technologies. These technological solutions should be examined and evaluated for a more widespread adoption within the IC where economically feasible. IC technological initiatives underway at entities like In-Q-Tel and IARPA appear to be making positive strides in developing, or funding potentially invaluable commercial technologies that meet the future OSINT demands of IC analysts of the future. Although individual efforts and technological successes have been noted at a variety of IC agencies, widespread success for OSINT across the IC enterprise remains an elusive target.

The IC set out to answer significant OSINT issues in 2006 with the establishment of the 2006 NOSE OSINT vision. The IC invested many resources and initiatives to effectively build OSINT capabilities through the implementation of tools and technologies. Some of these tools and technologies outlined in the original NOSE OSINT vision, namely OSCAR-MS and the OSC main Web site www.opensource.gov, actually met their mark.

Some individual IC agency contributions to the improvement of OSINT deserve to be shared throughout the IC, including the adoption of tools and technologies determined to have the greatest impact on the IC analyst's ability to see through the mountains of information and digest the portions of which prove valuable to a particular intelligence question, or issue. However, Treverton and Gabbard (2008) noted that there was no good IC-wide mechanism in to establish technological requirements or solicit technological needs that would apply across the IC:

> The most obvious problem is that there is no good, Community-wide mechanism to solicit analytic tool "needs" or to establish requirements. Although there are multiple sponsors for technology, in the CIA and beyond it in the wider community, those sources or sponsors are mostly uncoordinated. (Treverton & Gabbard, "Assessing the Tradecraft", 2008, p. 19)

Further, their study suggested a disconnect between the developers and users and how the tools are used (2008, p. 21). Has the IC begun to fully examine today's analytical requirements in today’s more demanding IC to determine the future technological initiatives necessary to aid analysts in sifting through the mountains of information now available within the global information environment?

Outside of developing IC-wide applications to be used against the deluge of data expected in the new cloud computing environment, information remains scarce on how the IC will drive future technological innovations to meet changing analytical requirements. To answer these questions in the future, readers will need to examine future technological developments and the enduring and future IC initiatives to see if the IC incorporates feedback or evaluative processes to ensure IC-wide best practices and procedures in implementing IC-wide tools and technologies in support of OSINT efforts.

Of course, cultural limitations as outlined in Chapter 4 have thus far thwarted substantive and systemic OSINT changes. The IC is going about its business much as before, and settling on the OSINT it is provided mostly from OSC efforts, or created from a variety of sources, by a variety of producers. New OSINT initiatives will continue to compete with traditional intelligence missions, as agencies will be forced to expend monies to accomplish IC ITE initiatives to stay in the current information technology cycle. In the coming years, increased competition for IT dollars to promote OSINT tools and technologies will likely face steep challenges as the IC faces an uncertain fiscal future. Whether IC agency-centric initiatives for the improvement of OSINT compete well against core missions in the coming years remain to be seen.

Analysts within the IC may not even realize that OSINT hasn’t lived up to the expectations of several decades of suggested reform efforts, and more recently the idea that OSINT’s stature within the IC should be better developed, and improved through a systematic, and concentrated effort. Where an IC analyst works largely determines their views, reliance, access to technologies, and their bias toward OSINT. Some IC analysts may not even realize what it was like even a decade ago when OSINT's worth was on the rise; during their tenure in the IC, the vast majority of OSINT has always been provided by the OSC, found in one of the many IC repositories, or even created and produced as required by individual analysts to meet mission requirements.

Conclusion

Nearly a decade ago, the WMD Commission Report (2005) found that the IC needed to change the way it conducted business and outlined a number of concrete recommendations. The report also spelled out that the IC was too slow to change and behind in applying "…cutting edge technologies…" (Report to the President of the U.S., 2005, p. 5). The report also called for the IC to be more nimble to the changing threat environment and to catch up on the pace of technological changes in today's environment. However, today, the IC is filled with a plethora of information technologies which often vary from agency to agency. Systemic technological changes in the ways the IC constructs its technological infrastructure are in their infancy as part of the IC ITE program, along with the move to cloud computing. Big data and social media seem to represent the future direction for OSINT within the IC. The future of OSINT within the IC may very well rest in how well the IC cloud is constructed, and how well the IC develops or acquires future applications, and tools and technologies to provide analysts the help they require to make sense out of big data.

However, as noted previously, commercial efforts at harnessing the power within big data provide valuable insights in that technological solutions to solving information issues may pose serious challenges. Whether the move to cloud computing will truly address important OSINT issues, especially issues surrounding information overload, remains to be seen. Movement to the cloud, with the aggregation of data may compound the problems associated with information overload. After the move to the cloud, the IC will proceed with caution and early IC initiatives will likely focus on ensuring that previous capabilities are not lost before proceeding further. The IC may make significant future progress in OSINT, however, little information may slip into the literature to suggest their successes due to the nature of sources and methods and classification requirements.

The literature suggests that OSINT still warrants attention within the IC. This examination also brings to light the difficulty in determining the best tools and technologies to watch in the future; these determinations will necessarily be predicated on what the IC wants OSINT to be, and to do. In the future, the OSC will continue to adapt to the changing information environment to fulfill its charter as a main producer of OSINT for the community. Whether new technological innovations will fundamentally change the OSC, or the IC efforts against OSINT, will long remain a question.

Maybe the notion of "fixing" of OSINT is a goal beyond the capabilities of the IC. Continual changes in the global information environment will likely make it difficult for the IC to ever catch up on the challenges presented by the deluge of big data. Perhaps the IC will never get a handle on information overload, and instead will continue to concentrate on information sources that have proven successful and valuable thus far. According to perhaps the most vocal OSINT advocate ever, Robert Steele wrote in 2003 that "no single nation, and certainly no single intelligence organization, is capable of single-handedly mastering the data acquisition, data entry, and data translation or data conversion challenges associated with 24/7 ‘global coverage” ("Information Peacekeeping & The Future of Intelligence," 2003, p. 202). Nance noted 20 years ago that we needed to adapt to the information technology cycle or be left behind (Nance, 1994). Maybe the future for OSINT within the IC, with its current practice of a de-centralized and distributed model for OSINT acquisition and production, will look much like the past.

Despite all of the rhetoric, reform recommendations, proposed OSINT initiatives and “implemented technological solutions” thus far, to quote a famous baseball player, Yogi Berra, “It’s like déjà vu all over again” (Knapel, 2011). After 9/11, OSINT’s stature within the IC reached its peak, although its importance had always been noted throughout the history of the IC. Numerous government commissions, reform efforts, independent studies, OSINT experts and proponents have recommended that we as a nation should produce more OSINT and use it more effectively within the IC. The information revolution has dictated that technological solutions are a necessary part of the solution to effectively deal with big data, and have long been a recommended solution for the IC to capitalize on the growing amounts of potential OSINT. Information overload has overwhelmed the IC, and few systemic changes have been made since 9/11. Changing global threats continue to change the types of questions that the IC must answer on a daily basis, and current world events seem to suggest this will likely persist for some time. Yet the IC finds itself some 10 years after the findings of the IRPTA and the WMD Commission largely faced with the similar questions of the past in regards to OSINT.

To ask again - Why haven't technologies fixed OSINT? Perhaps we should focus within the organizations, culture, people, processes, biases, and other constraints of the large socio-technical system that is the IC. Focusing only on technological solutions only address part of the problem for OSINT; solving OSINT issues will require an approach that addresses both the organizational and cultural aspects of the IC, in addition to its technological aspects. Until this is realized by decision makers within the IC, OSINT efforts will likely continue to not live up to their full potential, and the system itself may be impeding its future promise. Only then will it be possible for real OSINT solutions to take hold and begin to address the opportunities for OSINT in the changing requirements of today's IC.

The IC performs a valuable mission for the nation. The IC's main job is to provide information to the decision makers, from the war-fighter all the way up to the POTUS, based on the best intelligence possible. Often the intelligence answer to pressing requirements can at least be partially answered through OSINT. The nation's security is at stake. Let's hope the next intelligence failure doesn't stem from the lack of notable progress in building capabilities to acquire and effectively use OSINT in intelligence analysis. It's just too important to not get OSINT right this time.

Further Research

Further research will be necessary to fully examine how on-going IC initiatives address the myriad of OSINT issues and these are only a few of the many questions that come to mind. The first identified ICITE initiatives are scheduled to be implemented by 2017. The author would recommend that the IC revisit the state of OSINT in 2017 to see if the inherent technological improvements have made a significant difference for

OSINT, or in general, the ways in which analysis is conducted within the IC. Further, additional research will be necessary to examine the prevailing views of OSINT within the IC. It will be especially important to examine IC member views on OSINT after the ICITE meets its initial milestones.

Anther interesting issue that requires further examination includes the outcomes of the long-standing approach in trying to build OSINT experts throughout the IC. Many of the solutions offered, and as noted in Chapter 2, focused on addressing the human factors to improve OSINT. It would be an interesting question to answer in how well this approach has worked over the last 10 years.

It would also be interesting to examine what direction the next DNI takes OSINT within the IC. In an era of uncertain fiscal realities, a future of examination of how well OSINT holds up in comparison with traditional intelligence disciplines would be necessary to understand how well OSINT competes.

Further research will also be required to examine private sector and commercial technologies developments and their potential application with the IC to solve OSINT issues. Another revolves around understanding the impact of a younger, more technologically savvy workforce. Did their efforts influence technology within the IC, particularly for OSINT?

Appendix A - List of Abbreviations

Abbreviation	Full Description
ADDNI/OS	Assistant Deputy Director for National Intelligence Open Source
ATP	Army Techniques Publication
CEO	Chief Executive Officer
CI	Competitive Intelligence
CIA	Central Intelligence Agency
CIO	Chief Information Officer
COSPO	Community Open Source Program
COTS	Commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency
DCGS	Distributed Common Ground System
DCI	Director of Central Intelligence
DDCI	Deputy Director of Central Intelligence
DDNI	Deputy Director of National Intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIRNSA	Director of the National Security Agency
DNI	Director of National Intelligence
DoD	Department of Defense
ELINT	Electronic Intelligence
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FISINT	Foreign Instrumentation Signals Intelligence
FM	Field Manual
FMSO	Foreign Military Studies Office
GEOINT	Geospatial Intelligence
GIE	Government Intelligence Enterprise
HUMINT	Human Intelligence
I&W	Indications and Warning
IARPA	Intelligence Advanced Research Project Activity
IC	Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
IE	Intelligence Enterprise
IMINT	Imagery Intelligence
INSA	Intelligence and National Security Alliance
IRPTA	Intelligence Reform Act to Prevent Terrorist Attacks
IT	Information Technology
LNI	Library of National Intelligence
MASINT	Measurement and Signatures Intelligence
MIP	Military Intelligence Program
NASIC	National Air & Space Intelligence Center
NDAA	National Defense Authorization Act
NGA	National Geospatial-Intelligence Agency
NIC	National Intelligence Council
NIP	National Intelligence Program

Abbreviation	Full Description
NOSC	National Open Source Committee
NOSE	National Open Source Enterprise
NOSSAP	National Open Source Strategic Action Plan
NSA	National Security Act
NVTC	National Virtual Translation Center
ODNI	Office of the Director of National Intelligence
OSA	Open Source Academy, Open Source Center
OSC	Open Source Center
OSCAR-MS	Open Source Collection Acquisition Requirements Management System
OSI	Open Source Information, pre-dates OSINF
OSINF	Open Source Information
OSINT	Open Source Intelligence
OSIS	Open Source Information System
POTUS	President of the United States
SIGINT	Signals Intelligence
U.S.	United States
USG	United States Government
WBIL	World Basic Information Library
WMD	Weapons of Mass Destruction
WWW	World Wide Web

References

109th U.S. Congress. (2006). National Defense Authorization Act for Fiscal Year 2006 (109-163). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-109publ163/html/PLAW-109publ163.htm

2009 U.S. Army Posture Statement Document and Media Exploitation. (2009). Retrieved March 2014, from http://www.army.mil/aps/09/information_papers/document_media_exploitation.html

Ackerman, G., James, M., & Getz, C. T. (2007). The application of social bookmarking technology to the national intelligence domain. *International Journal of Intelligence & Counterintelligence*, *20*(4), 678-698. doi:10.1080/08850600701249808

Ackerman, R. K. (2006). Signal; intelligence center mines open sources.(central intelligence agency .open source center to maintain classified information).*60*, 51(4).

Are You Ready? Implications of a Changing Global Information Environment for Open Source Intelligence. (2001, July 1). Retrieved June 7, 2014, from http://www.oss.net/dynamaster/file_archive/090916/6e2588a3d13c9db47d49d9c23b464d79/Are You Ready.pdf

Barlow, J. P. (2002). Why spy? *Forbes, 170*(7), 42-47. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=ofm&AN=503938327&site=eds-live&scope=site&authtype=ip,uid

Baxter, G. (2011). Handbook of Socio-Technical Systems Engineering. Retrieved from http://archive.cs.st-andrews.ac.uk/STSE-Handbook/

Bean, H. (2007). The DNI's open source center: An organizational communication perspective. *International Journal of Intelligence and CounterIntelligence, 20*(2), 240-257.

Bean, H. (2014). The paradox of open source: An interview with douglas J. naquin. *International Journal of Intelligence & Counterintelligence, 27*(1), 42-57. doi:10.1080/08850607.2014.84279

Belko, M. (2004). *GOVERNMENT VENTURE CAPITAL: A CASE STUDY OF THE IN-Q-TEL MODEL* (Master's thesis). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a423132.pdf

Best, R. (2006). Intelligence Issues for Congress. Order Code IB10012. Congressional Research Service: Report.

Best Jr., R. A., & Cumming, A. (2007). Open source intelligence (OSINT): Issues for congress: RL34270. *Congressional Research Service: Report.*, 1. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=edb&AN=28445813&site=eds-live&scope=site&authtype=ip,uid

Best, R. A., & Cumming, A. (2008). *Open Source Intelligence (OSINT): Issues for Congress* (RL34270). Retrieved from http://assets.opencrs.com/rpts/RL34270_20080128.pdf

Best, C. (2008). Web mining for open source intelligence. Paper presented at the *Information Visualisation, 2008. IV'08. 12th International Conference,* 321-325.

Betts, M. (1994). Computerworld; agents spy internet data. (US intelligence agencies will use the internet) (surfing the internet).*28,* p1(2).

Braun, S. (2014, March 10). U.S. intelligence officials to monitor federal employees with security clearances | The Rundown | PBS NewsHour. Retrieved from http://www.pbs.org/newshour/rundown/us-intelligence-officials-monitor-federal-employees-security-clearances/

Brown, H. (1996). *Preparing for the 21st Century: An Appraisal of U.S. Intelligence; The Aspin-Brown Commission Report*. Commission on the Roles and Capabilities of the United States Intelligence Community.

Brown-Syed, C. (2011). Library and information studies and open-source intelligence. *Library & Archival Security*, *24*(1), 1-8. doi:10.1080/01960075.2011.551935

Cardillo, R. (2010). Intelligence Community Reform - A Cultural Evolution. *Studies in Intelligence*, *54*(3), 1-7. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/

Cardillo, R. (2012, July 1). Geospatial Intelligence Forum Interview with Robert Cardillo (H. Donnelly, Interviewer). Retrieved from http://www.dni.gov/index.php/newsroom/speeches-and-interviews/99-speeches-interviews-2012/580-geospatial-intelligence-forum-interview-with-robert-cardillo

Carroll, J. M. (2005). OSINT analysis using adaptive resonance theory for conterterrorism warnings. Paper presented at the *Artificial Intelligence and Applications*, 756-760.

Clapper, J. R. (1994). *Challenging joint military intelligence* (1994). JGQ Spring 1994. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=edsoai&AN=edsoai.832096591&site=eds-

live&scope=site&authtype=ip,uid; http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA528900

CIA Web Site — Central Intelligence Agency. (n.d.). Retrieved from http://www.cia.gov

Central Intelligence Agency. (2001, July). *Are you ready? Implications of a changing global information environment for open source intelligence*. Retrieved May 2014, from http://www.oss.net/dynamaster/file_archive/090916/6e2588a3d13c9db47d49d9c23b464d79/Are%20You%20Ready.pdf

Clark, C. S. (2012, November 12). *Intelligence community must adapt to era of vast data, study says - Defense - GovExec.com*. Retrieved from http://www.govexec.com/defense/2012/11/intelligence-community-must-adapt-era-vast-data-study-says/59886/

Clift, A. D. (2003). Intelligence in the Internet Era. *Studies in Intelligence*, *47*(3), 73-79. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol47no3/pdf/v47i3a06p.pdf

Dandar Jr., E. F. (1997). Meeting the open-source acquisition and exploitation challenge. *Military Review*, *77*(2), 30. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=f5h&AN=3207074&site=eds-live&scope=site&authtype=ip,uid

De Borchgrave, Arnaud. (2007). Commentary: Intelligent intelligence. *UPI International Intelligence*, Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=n5h&AN=1HTO790078417&site=eds-live&scope=site&authtype=ip,uid

Department of the Army. (2012). *Open Source Intelligence* (ATP 2-22.9). Retrieved from http://armypubs.army.mil/doctrine/30_Series_Collection_1.html

Director of Central Intelligence Directive 2/12 - Community Open Source Program. (n.d.). Retrieved April 2014, from http://www.fas.org./irp/offdocs/dcid212.htm

Discovery of Osama Bin Laden Result of Improved Information Sharing Amongst Intelligence Analysts. WASHINGTON. (2011, May 5). PRNewswire-USNewswire

Egan, K. (2005). The national virtual translation center. *Military Intelligence Professional Bulletin*, *31*(4), 64. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=f5h&AN=23190356&site=eds-live&scope=site&authtype=ip,uid

Fast, B. G. (2005). Always Out Front. *Military Intelligence Professional Bulletin*, *31*(4), 2-4.

Friedman, R. S. (1998). 'Open source intelligence (electronic version)'. *Parameters*, *28*, 129-165.

Fryer-Biggs, Z. (2014, March 7). Intelligence Agencies Ask for 5 Percent Less in 2015 | C4ISR & Networks | c4isrnet.com. Retrieved from http://www.c4isrnet.com/apps/pbcs.dll/article?AID=2014303060002

Fuld & Company. (2006). *The Global Leader in Competitive Intelligence Fuld + Company. Risk and Reward with Intelligence Technology. Intelligence Software Report 2006/2007*. Retrieved August 2006, from http://www.fuld.com

Gannon, J. C. (2000). Strategic use of open source information: A corporate strategy that leverage the best practices. *Vital Speeches of the Day*, *67*(5), 153-157.

Glasser, S. (2005, November 25). Probing Galaxies of Data for Nuggets. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2005/11/24/AR2005112400848.html

Goodwin, J. (2014, January 13). Office of Navy Intelligence to buy SMART.neXt messaging system support from Northrop Grumman. Retrieved from http://intelligencecommunitynews.com/2014/01/13/office-of-navy-intelligence-to-buy-smart-next-messaging-system-support-from-northrop-grumman/

Graham, M. (2007, July 17). Remarks and Q&A by the Deputy Director of National Intelligence for Collection Mrs. Mary Margaret Graham. Retrieved from http://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070717_speech_2.pdf

Greenberg, M. R., & Haass, R. (1996). *Making intelligence smarter: The future of US intelligence: Report of an independent task force.* Council On Foreign Relations.

Greenberg, A., & Mac, R. (2013, August 14). How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut - Forbes. Retrieved July 2014, from http://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/

Harris, D. (2014, May 2). DARPA is working on its own deep-learning project for natural-language processing — Tech News and Analysis. Retrieved July 2014, from https://gigaom.com/2014/05/02/darpa-is-working-on-its-own-deep-learning-project-for-natural-language-processing/

Hart, D., & Simon, S. (2006). Thinking straight and talking straight: Problems of intelligence analysis. *Survival (London, England), 48*(1), 35-59.

Howard, A. (2010, June 3). Connecting the dots with Intellipedia - O'Reilly Radar. Retrieved from http://radar.oreilly.com/2010/06/connecting-the-dots-with-intel.html

Iannotta, B. (2013, February 13). Intelligence Community transformation needs spending plan | Deep Dive Intel. Retrieved from http://www.deepdiveintel.com/2013/02/13/wanted-icite-acquisition-strategy/

IBM - Data analysis - i2 Analyst's Notebook. (n.d.). Retrieved June 10, 2014, from http://www-03.ibm.com/software/products/en/analysts-notebook

IC ITE – Doing in Common What is Commonly Done. (2013). Retrieved from Intelligence and National Security Alliance website: http://www.insaonline.org/i/d/a/Resources/ICITE_Doing.aspx

Information Peacekeeping & The Future of Intelligence. (2003). In J. B. De, W. Platje, & R. D. Steele (Eds.), *Peacekeeping intelligence: Emerging concepts for the future* (p. 202). Oakton, VA: OSS International Press.

Intelligence Authorization Act for Fiscal Year 1993. (1992). Washington, D.C.: [U.S. G.P.O.]:.

Intelligence Community Chief Information Officer. (2010, August). Intelink. Retrieved April 2014, from http://www.ndia.org/Divisions/Divisions/C4ISR/Documents/Breakfast%20Presentations/2010%20Presentations/Intelink%20Basic%20presentation.pdf

Intelligence Community Directive 301. (2006, July 11). Retrieved January 13, 2008, from http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-directives (since rescinded; found now at http://www.fas.org/irp/dni/icd/icd-301.pdf)

Intelligence and National Security Alliance. (2012, March). *ISSUU - Cloud Computing: Risks, Benefits, and Mission Enhancement for the Intelligence Community by Intelligence and National Security Alliance*. Retrieved May 2014, from http://issuu.com/insalliance/docs/insa_cloud_computing_2012_final/1?e=6126110/2711336

Intelligence and National Security Alliance. (2012, March). *Emerging Science and Technologies by Intelligence and National Security Alliance*. Retrieved May 2014, from http://issuu.com/insalliance/docs/emergingscience/1?e=6126110/1966904

Intelligence and National Security Alliance. (2012, October). *Expectations of Intelligence in the Information Age by Intelligence and National Security Alliance*. Retrieved May 2014, from http://issuu.com/insalliance/docs/rebalanceexpectations/1?e=6126110/2699361

Intelligence.Gov - Collaboration. Commitment. Courage. (n.d.). Retrieved March 2014, from http://www.intelligence.gov

INTellingence: Open Source Intelligence. (2010, July 23). Retrieved July 7, 2014, from https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

Intelligence Reform and Terrorism Prevention Act of 2004. (2004). Washington, D.C.: U.S. G.P.O.

Jardines, E. (2006, April). *National open source enterprise vision*. Retrieved Sept. 2008, from http://fas.org/irp/dni/osc/nose.pdf

Jardines, E. (2007, July). *ADDNI addresses ODNI open source conference*. Retrieved October 2007, from http://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070717_speech3.pdf

Kash, W. (2010, September 23). An interview with CIA Chief Technology Officer Gus Hunt -- FCW. Retrieved from http://fcw.com/articles/2010/09/27/feat-gus-hunt-cia-qanda.aspx

Kean, T., & Hamilton, L. (2004). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States: Official government edition.* (Official government ed.). Washington, D.C.: U.S. G.P.O.

Kernan, W. F. (2001). *NATO OSINT Handbook*. Retrieved from NATO website: http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

Kipp, J. W. (2005). Military intelligence professional bulletin; FMSO-JRIC and open source intelligence: Speaking prose in a world of verse.(foreign military studies office)(joint reserve intelligence center).*31*, 45(6).

Knapel, R. (2011, April 7). Yogi Berra: 'It's Deja Vu All Over Again' and His 25 Greatest Quotes | Bleacher Report. Retrieved from http://bleacherreport.com/articles/657044-yogi-berra-its-deja-vu-all-over-again-and-his-25-greatest-quotes

Lahneman, W. J. (2010). The need for a new intelligence paradigm. *International Journal of Intelligence and CounterIntelligence, 23*(2), 201-225.

Lazer, D. (2014, April 23). The Failure of Google Flu Trends Shows That Big Data Needs a Rethink | MIT Technology Review. Retrieved from http://www.technologyreview.com/view/526416/mistaken-analysis/

Lowenthal, M. M. (1999). Open Source Intelligence: New Myths, New Realities. *Intelligencer*, *10*(1), 7-9. Retrieved from http://www.oss.net/dynamaster/file_archive/040319/ca06aacb07e5cb9f25f21babf7ef2bf0/OSS1999-P1-08.pdf

MacDonald, M. S.O. ,Anthony G. (2002). Information overload. *Harvard International Review, 24*(3), 44. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=f5h&AN=7238067&site=eds-live&scope=site&authtype=ip,uid

Madill, D. L. (2005). Producing intelligence from open sources. *Military Intelligence Professional Bulletin*, *31*(4), 19-26.

McConnell, J. (2007). *100 Day Plan: Integration and Collaboration*. Retrieved from United States Intelligence Community website: http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/100_Day_Plan.pdf

McConnell, J. (2007, July). *DNI addresses ODNI open source conference*. Retrieved January 2008, from http://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070717_speech.pdf

McConnell, J. M. (2007). Overhauling Intelligence. *Foreign Affairs*, *86*(4), 49-58. Retrieved from http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20070619a_release.pdf

McLaughlin, J. E. (2001). *DDCI Remarks at Conference on CIA's Analysis of the Soviet Union — Central Intelligence Agency*. Retrieved from Central Intelligence Agency website: https://www.cia.gov/news-information/speeches-testimony/2001/ddci_speech_03092001.html

Mercado, S. (2004). Sailing the sea of OSINT in the information age (2004). 2004. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=edsoai&AN=edsoai.832092466&site=eds-live&scope=site&authtype=ip,uid; http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA525400

Metz, C. (2003, July 1). Software: Text Mining - The Future of Technology | PCMag.com. Retrieved August 2014, from http://www.pcmag.com/article2/0,2817,1130911,00.asp

Miller, J. (2013, September 10). Intel Community offers first glimpse of future IT tools, network - FederalNewsRadio.com. Retrieved from http://www.federalnewsradio.com/411/3447343/Intel-Community-offers-first-glimpse-of-future-IT-tools-network-

Mohammed, A., & Goo, S. K. (2006, June 15). Government increasingly turning to data mining. The Washington Post, p. D3.

Nance, Mick. (1994). *The Generation Gap: Open-Source Information, Intelligence, and the Government*. NATIONAL WAR COLLEGE, WASHINGTON DC.

National Open Source Committee. (2009). *National Open Source Strategic Action Plan*. Retrieved from Federation of American Scientists website: http://www.fas.org/irp/dni/osc/nossap.pdf

National security act of 1947. (2009). Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=f5h&AN=21212825&site=eds-live&scope=site&authtype=ip,uid

Nolan, P. (2012). A Curator Approach to Intelligence Analysis. International Journal of Intelligence and CounterIntelligence, 25(4), 786-794. Retrieved from http://dx.doi.org/10.1080/08850607.2012.678698

Pagliery, J. (2014). *The deep web you don't know about*. CNN Newsource Sales Inc. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=n5h&AN=BAQ41394108420&site=eds-live&scope=site&authtype=ip,uid

Peak, D. (2005). Military intelligence professional bulletin; DOD and the DNI open source center--building the partnership.(department of defense)(director, national intelligence).*31*, 15(3).

Pingdom. (2013, January). *Internet 2012 in numbers*. Retrieved April 2014, from http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/

Report to the President of the United States (Official government ed.). (2005). Washington, D.C.: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

Rolington, A. (2006). Objective intelligence or plausible denial: An open source review of intelligence method and process since 9/11. *Intelligence and National Security, 21*(5), 738-759.

Rosenberg, B. (2012, March 13). Intelligence community strengthening its links, with DIA taking the lead on the desktop environment -- Defense Systems. Retrieved April 2014, from http://defensesystems.com/Articles/2012/02/28/Chief-View-Grant-Schneider-DIA.aspx?p=1

Rosenbush, S., & Totty, M. (2013, March 10). How Big Data Is Changing the Whole Equation for Business. Retrieved from http://online.wsj.com/news/articles/SB10001424127887324178904578340071261396666

Rothkopf, D. (2005). Technology can fix U.S. intelligence. *Technology Review*, *108*(2), 34-34. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=bth&AN=16017766&site=eds-live&scope=site&authtype=ip,uid

Saunders, K. A. (2000). *Open Source Information: A True Collection Discipline* (Master's thesis, Royal Military College of Canada).

Shachtman, N. (2010). Exclusive: Google, CIA invest in 'Future' of web monitoring. *Danger Room. Wired.*

Sheets, D. B. (2013). Social media and open-source intelligence resources for the modern foreign area officer. *FAOA Journal of International Affairs, 16*(2), 5-9. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=mth&AN=93288757&site=eds-live&scope=site&authtype=ip,uid

Shrader, K. (2005, November). New U.S. Intel Center Studies Free Secrets. Retrieved March 2014, from http://www.washingtonpost.com/wp-dyn/content/article/2005/11/08/AR2005110801250.html

Socio-technical systems. Baxter, G. (2011). http://archive.cs.st-andrews.ac.uk/STSE-Handbook/SocioTechSystems. In *LSCITS Socio-Technical Systems Engineering Handbook*. University of St Andrews. http://archive.cs.st-andrews.ac.uk/STSE-Handbook/

Studeman, W. O. (1993). Teaching the giant to dance: Contradictions and opportunities in open source information. *Competitive Intelligence Review, 4*(1), 25-29. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=bth&AN=10444633&site=eds-live&scope=site&authtype=ip,uid

Symposium Speakers Define Strategic Plan For Using Open Source Intelligence. (1992). U.S. Newswire.

Tarasiuk, A. (2009, October 20). Intelligence Community Chief Information Officer Panel, 2009 GEOINT Symposium San Antonio, Texas. Retrieved from http://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20091020_speech.pdf

Travers, R. (1999). *The coming intelligence failure* (1997). 1997. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=edsoai&AN=edsoai.832095166&site=eds-

live&scope=site&authtype=ip,uid; http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA527323

Treverton, G. F. (2005). *The Next Steps in Reshaping Intelligence*. Retrieved from Rand Corporation website: http://www.rand.org/content/dam/rand/pubs/occasional_papers/2005/RAND_OP152.pdf

Treverton, G. F., & Gabbard, C. B. (2008). *Assessing the Tradecraft of Intelligence Analysis*. Retrieved from Rand Corporation website: http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR293.pdf

Turbiville, Jr., Graham H. Prinslow, Karl E., WALLER (1999). Assessing emerging threats. *Military Review*, *79*(5), 70. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=f5h&AN=2651146&site=eds-live&scope=site&authtype=ip,uid

U.S. National Intelligence - An Overview 2013 - Sponsored by the Intelligence Community Information Sharing Executive. (2013, April). Retrieved March 2014, from http://www.dni.gov/index.php/newsroom/reports-and-publications/193-reports-publications-2013/835-u-s-national-intelligence-an-overview-2013-sponsored-by-the-intelligence-community-information-sharing-executive

Vision 2015: A Globally Networked and Integrated Intelligence Enterprise. (2008). Retrieved from Director of National Intelligence website: http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Vision_2015.pdf

Vivisimo Gets NSF Data Contract For Homeland Security. (2003, June 12). Retrieved April 2014, from http://www.spacedaily.com/reports/Vivisimo_Gets_NSF_Data_Contract_For_Homeland_Security.html

Wailgum, T. (2008, October 6). Extreme makeover: The CIA edition - CIO New Zealand. Retrieved from http://www.cio.co.nz/article/469808/extreme_makeover_cia_edition/

Wait, P. (2006, March). Intelligence Units Mine the Benefits of Public Sources: Open Source Center Draws, Analyzes Info from a Variety of Public Databases. Retrieved July 2007, from Government Computer News, 20 March 2006. URL: http://www.gcn.com/print=25_6/40152-1.html

Warner, B. (2013, February 5). What the Intelligence Community Is Doing With Big Data - Businessweek. Retrieved April 2014, from http://www.businessweek.com/articles/2013-02-05/what-the-intelligence-community-is-doing-with-big-data

Warner, M., & McDonald, J. K. (2005, April). *US Intelligence Community Reform Studies Since 1947*. Retrieved September 2008, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/US%20Intelligence%20Community%20Reform%20Studies%20Since%201947.pdf

Weinberger, S. (2011). Spies to use twitter as crystal ball. *Nature*, *478* (7369), 301-301. doi:10.1038/478301a

What Is Open Source Information? (1993). Tactical Technology, 3(1). 6 January 1993.

Williams, C. (2011). 'Google effect' hits spies. *Daily Telegraph (London)*, , 9-9. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=n5h&AN=8Q253734940&site=eds-live&scope=site&authtype=ip,uid

Wright, L. (2008). A REPORTER AT LARGE the spymaster the new director of national intelligence has a controversial plan to tighten national security. *New Yorker -New Yorker Magazine Incorporated-*, , 42-59. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=edsbl&AN=RN222573062&site=eds-live&scope=site&authtype=ip,uid

Yasin, R. (2012, March 13). Can cloud improve intelligence community's big data analysis? INSA white paper says yes. -- GCN. Retrieved from http://gcn.com/articles/2012/03/13/intelligence-community-cloud-big-data-analysis.aspx

YOUNG, A. (2013). Too much information. *Harvard International Review, 35*(1), 24. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=f5h&AN=87979388&site=eds-live&scope=site&authtype=ip,uid