GOING BEYOND APPLES TO ORANGES: OPEN SOURCE INTELLIGENCE AND UNITED STATES NATIONAL SECURITY DECISION-MAKING

A Thesis Submitted to the International Relations Program of Tufts University

By

NICHOLAS G. GIURLEO

In Partial Fulfillment of the Requirements for the Degree of a Bachelor of Arts in International Relations

2018-2019

In Loving Memory of my Grandfathers:

GENNARO ANDRIANI (1930-2012)

and

NICODEMO "NICK THE TAILOR" GIURLEO (1942-2013)

This Thesis is Dedicated.

ACKNOWLEDGEMENTS

Before I delve headfirst into the exciting world of intelligence and national security, let me begin with a few acknowledgements.

I would first like to thank Tufts University, especially the Tufts International Relations Program, for giving me the chance to write a thesis for my major. I never intended on writing an undergraduate thesis, but here I stand today, 150 pages and countless hours of intensity, pacing, and exhaustion later, submitting my *magnum opus* for review. I'll never forget the day I decided to commit myself to the challenge of writing a thesis. It was a beautiful, sunny, late spring day in Bologna, Italy. I was pensively wandering the streets of that medieval city when one-way or another open source intelligence came to mind. I thought to myself, "that'd be an interesting idea for a thesis." I wondered if it was too late to submit a prospectus. That evening I looked up the deadline date on my computer: I had two-days. After a deep sight, I knew what I had to do. I opened a Word document and began typing. Over a year later, I can finally say I've stopped typing. I can also say that I'm a masochist and that an easy "senior spring" never came to mind even once.

I would also like to thank my thesis advisor, Professor David Ekbladh, for not only accepting my late request for an advisor but also for being an invaluable source of aid, advice, and friendship throughout the entire process. Professor Ekbladh went out of his way to do all that he could to keep me on track and help me in my travels down the many winding and lonely roads of writing the thesis. For his help and support, I am infinitely grateful.

I also thank Professor Jeff Taliaferro, the other member of my thesis committee, for taking time out of his busy schedule to carefully scrutinize my words on all things intelligence and national security. I thank the research librarians and general staff of the Tisch Library and of the Ginn Library, as well as the research assistants at the John F. Kennedy Presidential Library and Museum, for their aid in finding Cuban Missile Crisis intelligence documents.

I would especially like to thank my family and friends for their moral support. I thank my mother Marianne, my father Nick, and my sister Natalie for putting up with my mad, unintelligible ravings about "the thesis" and being supportive of my ambitious

project. I thank my extended family as well for their encouragement. I would be remiss not to thank my friend Attorney Bill Barabino for both employing me and challenging me everyday to go above and beyond my potential as a legal and political thinker.

Lastly, and most importantly, I thank God for the education I am very blessed to be receiving here at Tufts University in the country that, no matter what I say in today's political climate, I still love.

Nick Giurleo
Medford, 2019

CONTENTS

INTRODUCTION

We are in the midst of an "open source" revolution, a transformation driven by the unprecedented degree to which the twenty-first century world finds itself technologically interconnected.[1]

Indeed, the revolution in information technology, commerce, and politics since the Cold War's end is only making "open" or publically available information more accessible, ubiquitous, and valuable than ever before.[2] From the liberties of the Internet to the twenty-four seven production of news and social media content, the sheer quantity of open source information (OSINF) has exploded in recent years.

There is reason to believe the effective exploitation of OSINF can play an essential role in giving the national security community as a whole insight and context at a relatively low cost.[3]

For example, researchers at the Middlebury Institute of International Studies' nonproliferation center were recently able to use OSINF to confirm reports that North Korea had tested another solid-fuel missile engine.[4] Using Google Earth, lead researcher Dave Schmerler and his team were able to make three dimension models of buildings in North Korean photos and use media reports of where North Korean dictator Kim Jong Un

[1] Stevyn D. Gibson, "In the Eye of the Perfect Storm: Re-imagining, Reforming and Refocusing Intelligence for Risk, Globalisation and Changing Societal Expectation," *Risk Management: An International Journal* 7, no. 4 (2005): 24. Gibson writes, "Postmodern society…can usefully be related to the invention of the Internet and the broader late-20th century transformation in information and computer technology…exemplified by the PC, the mobile phone, satellite TV and digital technology."
[2] Stephen Mercado, "Sailing the Sea of OSINT in the Information Age: A Venerable Source in a New Era," *Central Intelligence Agency Library* 48, no. 3 (2004).
[3] "INTelligence: Open Source Intelligence," *Central Intelligence Agency: Featured Story Archive*, (Washington, D.C.), August 6, 2018.
[4] Anna Fitfield, "With technology, these researchers are figuring out North Korea's nuclear secrets," *The Washington Post* (Washington, DC), Nov. 21, 2017.

made public appearances to identify the exact building where the test took place.

Amnesty International likewise conducted a study considering the role of OSINF in convincing policymakers in countries like the United States, the United Kingdom, and France to launch retaliatory missile strikes for Damascus's decision to authorize chemical weapons strikes in Syria on April 7, 2018.[5] Organizations like Amnesty International were able to use a wide range of photographs and videos from the incident to confirm the Syrian government's involvement in the attack. From this result, these NGOs have argued that, "in the digital age…open source content is increasingly central to states' public diplomacy, and even can inform decisions by international institutions." Furthermore, many have argued for the importance of OSINF in forming new routes to "justice and accountability" for the victims of atrocities in more remote areas of the world.

Both of these examples illustrate that with greater technological latitude, along with wider access to open sources—like photos and videos that can be captured by mobile devices and online services like Google Earth—OSINF can be exploited to draw conclusions pertaining to matters of national security. If organizations like Middlebury College and Amnesty International are able to utilize OSINF to achieve these results, what prevents the US government—particularly the United State Intelligence Community (IC)—from doing the same?

This thesis seeks to analyze this relationship between intelligence and national security decision-making, concentrating on the Open Source Intelligence discipline (OSINT). OSINT can be generally defined as publically available information that goes

[5] Sam Dubberley, "How open source evidence took a lead role in the response to the Douma chemical weapons attack," *Amnesty International* (Boston, MA), April 23, 2018.

through, in a timely manner, the intelligence cycle—a sequence of events consisting of collection, exploitation, analysis, classification, and dissemination used to produce finished products that policymakers may or may not choose to utilize in their decision-making considerations. One of the reasons analyzing the relationship between OSINT and national security decision-making is important is because an insufficient amount of scholarly attention has been paid to understanding this specific, but potentially important, and certainly intriguing, relationship. With information technologies becoming more advanced and interwoven into the communications fabric of the world, the future value of OSINT for intelligence studies will likely increase as these technologies continue to develop and become more ubiquitous. It is crucial that both policymakers and the US intelligence community understand the overall growing importance of the OSINT discipline and how it relates to national security decision-making.

The thesis will attempt to answer three correlational and policy analysis questions. Part One of the thesis will answer the first question. Part Two of the thesis will answer the second two questions:

1. What is the relationship, if any, between the Open Source Intelligence (OSINT) discipline and national security decision-making in the United States of America?
2. If the quantity and quality of open source information and finished open source intelligence products collected and produced respectively from the OSINT intelligence discipline *increases*, how does this impact national security decision-making?
3. If a causal relationship can be established between OSINT and national

> security decision-making, to what extent can it be established? When the *quantity* of OSINF/OSINT increases does national-security decision-making produce more optimal policy results? When *quality* increases does national security decision-making produce more optimal policy results? When quantity and quality *both* increase, does national-security decision making produce more optimal policy results?[6]

The thesis will be divided into two parts. Part One will attempt to develop a *theoretical* nexus on the relationship (if any) between the OSINT variable and the national security decision-making variable.

Chapter One will start by outlining the methodology to be utilized in Part One—defining the theoretical research question the thesis seeks to answer and addressing how the thesis will drawn conclusions on the fundamental relationship in question.

Chapter Two will review relevant literature on the broad topics of OSINT and national security decision-making, focusing on what scholars have written on the relatively novel topic of the OSINT discipline and what scholars have said on national security decision-making structures and optimal policy results.

Chapter Three will discuss the OSINT variable. The chapter begins by deconstructing the first variable: OSINT. It will first define OSINT, review its institutional history and then distinguish the discipline from its sub-component OSINF. The latter part of the chapter seeks to add to existing literature on OSINT by outlining

[6] Note that Chapters Six and Seven of the thesis will clarify what is meant by "optimal policy results" in the context of the Cuban Missile Crisis of 1962. For the purposes of Part One, the following definitions of *policy* ("a deliberate statement [of intent] aimed at achieving [a] specific objective…to solve existing challenges [and] problems in any society") and *optimal policy results* ("[when a] policy is addressing the [given] problem(s) and…[when its] implementation is proceeding effectively.") will be adopted going forward. See Kojo Appiah-Kubi, "Policy Making Process," PowerPoint, DRUSSA-ISSER Executive Training on 'Influencing Policy,' December 10, 2015, slides 2/32., 11/32.

three novel present and potential uses of the intelligence discipline. In doing so, the deconstructed OSINT variable will be reconstructed and considered in contexts in which it acts independently from the national security decision-making variable. The chapter will conclude by reviewing the above and beginning to establish the framework of open source intelligence's role (if any) in the US national security system.

Chapter Four will discuss the national security decision-making variable. The structure of this chapter will be as follows: (1.) a brief history of how the traditional "security" needs of the US transformed into a novel conception of "national security"; (2.) a deconstruction of the national security decision-making variable into its formal and informal components; and (3.) an explicit final statement on national security decision-making structures and their relationship with optimal policy results.

Chapter Five will recapitulate the major points of what was established in Chapters Three and Four and, in doing so, will deduce the relationship between OSINT and national security decision-making. The chapter will conclude by explicitly answering the Part One research question and beginning to discuss how the conclusions drawn in the chapter will be utilized in Part Two of the thesis to come.

Part Two of the thesis serves to apply the theoretical conclusions developed in Part One to a *quantitative case study* in which the OSINT variable and the national security decision-making variable were factors. The historical case study of analysis will be the Cuban Missile Crisis of 1962. The end purpose of this part of the thesis is to stack up the theoretical conclusions drawn in Part One against the quantitative conclusions drawn in Part Two to make a final, concluding statement on the relationship between the OSINT variable and the national security decision-making variable.

The second part begins with Chapter Six, an outline of specific methodology used to conduct the quantitative case study. This chapter will also begin to discuss how the theoretical perspective developed in Part One will be considered in light of the results produced from the quantitative test.

Chapter Seven begins with a brief contextual discussion of the intelligence and national security dimensions of the crisis, concluding with an exploration of the institutional history of FBIS between the years 1957 and 1967. The remainder of the chapter records the empirical results of the experiment.

The Conclusion of the thesis will be divided into two principle parts: the first will offer an analysis interpreting the quantitative results of the experiment as recorded in Chapter Seven. The second part—taking these results into consideration along with the theoretical conclusions drawn on the nexus between OSINT and national security decision-making as detailed in Chapter Five—will draw a final conclusion on the fundamental relationship between the OSINT variable and national security decision-making. This final chapter will also discuss potential future studies for considering the nexus between the OSINT variable and the national security decision-making variable.

PART ONE: NATIONAL SECURITY AND OPEN SOURCE INTELLIGENCE

"You must live in the present, launch yourself on every wave, find your eternity in each moment. Fools stand on their island of opportunities and look toward another land. There is no other land; there is no other life but this."

-Henry David Thoreau, *The Journal of Henry David Thoreau*, April 24, 1859

CHAPTER ONE: PART ONE METHODOLOGY

Part One of the thesis primarily seeks to consider the *theoretical* relationship between two different variables. This part of the thesis will answer the following research question:

> What is the relationship, if any, between the Open Source Intelligence (OSINT) discipline and national security decision-making [7] in the United States of America?

I will begin by considering each variable independently, in doing so, defining the variable and considering alternative known relationships of the variable to the main relationship the thesis wishes to address. The admittedly broad variables in consideration will be tested monolithically, but defined by deconstructing each into its respective constituent components and considering their relationship to other variables outside of the context of the other. For the case of OSINT, this will consist of: reviewing the history of the discipline; considering various existing definitions of the term OSINT; distinguishing OSINT from OSINF; and discussing the generational history and future of the discipline. For the national security decision-making variable, this deconstruction and analysis of other relationships will include: reviewing the historical evolution of national security in the US; considering the formal structures that constitute national security decision-

[7] Note that there are two different ways of considering the relationship between *policy* and national security decision-making. The first conception of national security decision-making sees national security decisions as being made *before* policymakers devise policies (i.e. the decisions policymakers make on the substance of policies they wish to create). The second conception sees national security decision-making occurring *after* policymakers devise policies (i.e. the decisions policymakers make to *implement* their policies). This thesis will focus on the first conception in the context of how *intelligence*, particularly OSINT, informs national security decision-making, but is primarily concerned with the relationship between the OSINT variable and the national security decision-making variable in the second conception. Part One of the thesis focuses on the first conception while Part Two of the thesis concentrates on the second.

making; considering the informal structures that make up national security decision-making; and considering existing models on national security decision-making in their relation to optimal policy results.

The above will be accomplished in Chapters Three and Four. Chapter Five will consider the nexus between the two variables previously discussed, concluding by explicitly answering the above question this part of the thesis seeks to answer. Part Two of the thesis will consider the conclusions drawn in Part One in quantitatively testing the relationship between the OSINT variable and the national security decision-making variable.

It is important to note that the Part One will be a qualitative analysis, whereas part two will be a quantitative and data-driven one. This qualitative part of the paper will synthesize general principals of OSINT and national-security decision making to answer the research question broadly. The purpose of this "theoretical" part of the paper is to develop a principle-based answer to the research question, that can be considered side-by-side with the empirical results that will be drawn from the second part of the thesis. The final conclusion of the thesis will compare the results from Part One and Part Two to make a final statement on the nexus (or lack thereof) between the OSINT variable and the national security decision-making variable.

CHAPTER TWO: LITERATURE REVIEW

Before beginning a substantial, theoretical discussion of the OSINT variable and the national security decision-making variable and their relationship or lack thereof, a literature review is first in order.[8]

National Security Decision-Making Literature

In order to understand the national security decision-making variable to be considered, it is essential to first establish how national security decisions are made in the US. This part of the literature review will present literature on two different theoretical perspectives on the structures of national security decision-making and their relationship to the production of more optimal policy results.

Institutionalism Produces Optimal Policy Results

Institutionalism has largely focused on the formal structures that define, facilitate, and oftentimes dictate national security decision-making in the United States. Some scholars, like Cyr[9], have argued against relying on the formal structure of the National Security Council in arbitrating decision-making. Cyr argues that there is no ideal approach to national security decision-making organization but that an institutional approach, generally speaking, produces more optimal policy results than any other approach. He makes the case for an increased role of the State Department in decision-making. He also proposes a three-pronged model for institutional national security

[8] A note on the notes: all sources referenced in this chapter will be cited in full. Sources that are repeated in the discussions of the chapters that follow will also be cited in full for reasons of avoiding unclear citation abridgements of those works procedurally cited from the literature review here in Chapter Two.
[9] Arthur Cyr, "How Important is National Security Structure to National Security Policy?", *World Affairs* 146, no. 2 (1983): 127-147.

decision-making: an "administrative approach", a "theoretical approach", and a "centralized dominance approach". He assigns dominant approaches to decision-making to the presidential administrations of Dwight Eisenhower, Richard Nixon, Jimmy Carter, and Ronald Reagan.

Kolodziej[10] explores the concept of optimal policy results from a historical perspective, considering how the formal, institutional structures of national security decision-making's change over time have contributed to prudent decision-making. He traces the origin of institutionalized policymaking to the Eisenhower iteration of the NSC and further makes the case that this institutionalism effectively encourages the overall rationale for US security and foreign policy.

Pfaltzgraff and Ra-anan[11] bypassed Cyr's rather unorthodox emphasis on a move away from the NSC as the primary source of institutionally based national security decision-making. These scholars are notable for their turn toward historical analysis—similar to that of Kolodziej's—of the national security system from a structural-historical perspective. They reach almost a legal level of analysis in discussing the significance of the 1947 National Security Act in informing, dictating, and producing optimal national security decision-making. Lord[12] adds to this line of scholarship with his discussion of the institutional foundations of the NSC. Lord distinguishes himself from Pfaltzgraff and Ra-anan by concentrating extensively on the importance of NSC *staff* in the institutional decision-making process. Lord laudably, but perhaps somewhat excessively, compartmentalizes the theoretical duties of NSC staff in his schematic.

---

[10] Kolodziej, Edward A. Kolodziej, "The National Security Council: Innovations and Implications," *Public Administration Review* 29, no. 6 (1969): 573-585.
[11] Robert L Pfaltzgraff Jr, and Uri Ra'anan, *National Security Policy: The Decision-making Process*, Hamden: Archon Books, 1984.
[12] Carnes Lord, *The Presidency and the Management of National Security*, New York: Free Press, 1988.

This thesis devotes substantial attention to one scholar's general modeling of national-security decision making: Newmann[13]. While the model Newmann proposes is flawed in ways Chapter Four of this thesis will later explicitly detail, Newmann's work deserves attention for its comparative analysis of the 1995 model of Walcott and Holt. Both Newmann and Walcott and Holt adopt a three-pronged model for national security decision-making that produces optimal policy results, emphasizing the importance of institutional structures, while not undermining the importance of idiosyncratic approaches to national-security decision-making in producing these same results. Newmann considers the administrations of Carter, George H.W. Bush, and Reagan in constructing his model.

The Idiosyncratic Approach Produces Optimal Policy Results

The impetuses for national security decision-making that go beyond the strictly institutional can be classified as idiosyncratic approaches to national-security decision-making. Whereas institutionally based theory on national security has been developed since the Second World War and the 1947 National Security Act, idiosyncratic theory is more of a recent phenomenon. Jablonsky et al.[14] for example, has looked to broader conceptions of national security decision-making, beyond the strictly institutional, that may contribute to the production of more optimal policy results. These scholars have importantly taken note of the three broad foundational principles of national security: national interests, security, and grand strategy in informing national security decision-making. In addition to a traditional structural history of the decision-making a scholar of

[13] William W. Newmann, "The Structures of National Security Decision Making: Leadership, Institutions, and Politics in the Carter, Reagan, and G.H.W. Years", *Presidential Studies Quarterly* 34, no. 2 (2004): 272-306.
[14] David Jablonsky, et al., *U.S. National Security: Beyond the Cold War*, Carlisle: U.S. Army War College Strategic Studies Institute Press, 1997.

institutionalism may posit, Jablonsky et al. connect these three broad principals to a new, broader view on national-security decision-making that goes beyond exclusively highlighting the importance of formal structures in contributing to more optimal policy results but to emphasizing the importance of informal structures in producing these results as well. Ray[15], like Cyr in some respects, questions the extent to which the formal, institutional structure of the NSC is the best means of countering external security threats to a state and producing optimal policy results. He argues that a post-Second World War political economy that redefined national security has undermined the institutional appeal of the NSC, a "stereotypical American institution."

Some scholars have considered these broad principles of idiosyncratic decision-making leading to optimal policy results individually and in more specific contexts. Kobb and Kraig[16] for example, consider "grand strategy" through the lens of policy decision-making during the Bush Administration's involvement in the wars in Iraq and Afghanistan. Other scholars like Watson[17] have likewise considered broad, nontraditional principles. While Watson includes a discussion of general security theory in her work, she also notably addresses what she calls "nontraditional threats" relating to national security –economically, environmentally, and socially—arguing that conceptions of grand strategy should take these unconventional realities into consideration.

Other scholars, like Weiss,[18] have attempted to explicate the idea that idiosyncratic national security decision-making leads to more optimal policy results in

[15] Aswini K. Ray, "Political Economy of the National Security Council," *Economic and Political Weekly* 25, no. 9 (1990): 424-426.
[16] Larry Kobb, and Michael Kraig, Winning the Peace in the 21st Century, Muscatine: Task Force Report, 2003.
[17] Cynthia Watson, *US National Security: A Reference Handbook, Second Edition*, Santa Barbara: ABC-CLIO, 2008.
[18] Linda Weiss, *The National Security State and Technology Leadership*, Ithaca: Cornell University Press, 2014.

even broader, more general ways. While Weiss was not the first scholar to make use of the umbrella term "national security state", her monolithic characterization of national security as a single entity is flawed. In her work, she provides a commendable historical record of the rise of national security apparatuses in the United States following the end of the Second World War, as well as a resonant discussion of the dangers of a "military industrial complex", but her national security state characterization misses the fundamental reality of national security in the United States—that institutional or "formal" structures *coexist* with idiosyncratic or "informal" structures.

One intriguing approach to the idiosyncratic elements of national security decision-making and optimal policy results one finds in Krebs.[19] Krebs devotes his work to a well-written and easy to follow discussion of a rather abstract concept: national security "narratives". He speaks positively of these narratives as deriving from the various schools of international relations theory that posit differing opinions on how national security decisions are made. While Krebs does not detail which theoretical school's narrative produces the most optimal policy results, he emphasizes the importance of narrative in forming cohesive models of national security decision-making. Krebs also importantly begins to explore the psychological elements and cognitive biases that influence the decision-making capabilities of leaders with national security decision-making power. Mintz[20] devotes himself more expressly to understanding these psychological elements and cognitive biases of decision-making that contribute to the creation of narratives. In his work, he explores poliheuristic theory, or theory that

[19] Ronald R. Krebs, *Narrative and the Making of US National Security*, New York: Cambridge University Press, 2015.
[20] Alex Mintz, "How do Leaders Make Decisions? A Poliheuristic Perspective", *The Journal of Conflict Resolution* 48, no. 1 (2004): 3-13.

attempts to bridge the gap between cognitive and rational theories of decision-making.

Many scholars moving away from exclusively institutional analysis have turned to these broader elements and biases of idiosyncratic national security decision-making explicitly. Some have argued that these broader elements and biases paradoxically lead to more optimal policy results for national security decision-making. Pfiffner[21], for example, provides a very useful secondary source compendium of the history of scholarly thought on rationality and national security decision-making. Pfiffner's choice of sources helps to fortify his derivative analysis of the origins of the idiosyncratic means by which much national security decision-making is made. In other words, he traces how the core idea behind the "rational actor" approach that forms the bedrock of institutionalism breaks down when the modern, inescapable decision-making realities of "advisory systems" and "multiple advocacy" incline decision-makers toward making decisions anywhere on the spectrum of unadulterated bias to optimal policy results/honest broker-backed decision-making.

Scholars like Holt[22] have specifically focused on the president as a national security decision-maker influencing the production of optimal policy results. Holt argues that due to the increasing "openness" of the modern presidency, the President of the United States faces an increased traffic of persuasive attempts by organized interests to influence decision-making. She makes the interesting, but perhaps somewhat exaggerated, case that rigid adherence to institutional national security structures leads to less optimal policy results. To conclude her argument, she makes five concrete policy

[21] James P. Pfiffner, "Presidential Decision Making: Rationality, Advisory Systems, and Personality", *Presidential Studies Quarterly* 35, no. 2 (2005): 217-218.
[22] Karen M. Holt, "Strengthening Presidential Decision-Making Capacity", *Presidential Studies Quarterly* 30, no. 1 (2000): 27-46.

recommendations to put the president "back in control" of presidential decision-making, which include integration of a more merit-based system of national security decision-making staff and advisers and less "noncareerists."

Open Source Intelligence Literature

Unlike the bounteous quantity of literature on national security decision-making, the literature on the OSINT discipline is much scarcer. Scholars have been writing about national security since before the Second World War. Scholars of intelligence of the open source variety only began writing on the potential of the open source movement and open source information during the late 1990s and early 2000s. There is a tremendous need for more studies and more literature on OSINT, particularly on the subject of its practical applications both within and beyond the US Intelligence Community.

That said, the purpose of this section of the literature review is to provide a brief compendium of historical and descriptive literature on OSINT. The next chapter of the thesis will both deconstruct the OSINT variable and consider the OSINT variable in an exclusively intelligence context. The works to be presented are works that deconstruct the constituent components of the OSINT discipline and discuss the role of OSINT in the Community at large.

Deconstructing OSINT and OSINT's Role in the US Intelligence Community

One of the most recent and comprehensive sources of general OSINT literature comes from Williams and Blum.[23] Their compendium of discussions on virtually every major topic related to the OSINT intelligence discipline is covered in this work,

[23] Heather J. Williams, and Illana Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, Boston: The RAND Corporation, 2018.

published for the RAND Corporation. Williams and Blum was enormously valuable to the thesis research process. The work provides a general outline of major OSINT issues, including: defining OSINT and OSINF; the stages of the standard OSINT intelligence cycle; the institutional history of the discipline; the internal divisions of OSINF; the role of commercial-off-the-shelf (COTS) tools for technical OSINT capabilities; and generationally defining OSINT and a potential third generation of the discipline.

Second to Williams and Blum, Best and Cumming[24] is one of the most informative sources on the general functioning and importance of OSINT available. Best and Cumming, writing jointly for the Congressional Research Service, provide a useful analysis of the normative value of open source information as well as a thorough history of the intelligence discipline. In ways Williams and Blum do not, Best and Cumming further expand the already lengthy dictionary of OSINT vocabulary. They also importantly note and analyze legislation and congressional reports with important OSINT implications, such as the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the 9/11 Commission Report of 2004, and the Iraqi WMD Report of 2005.

Not all scholarly literature on OSINT has approached the topic generally. Indeed, a considerable quantity of literature has focused on the technical aspects of OSINT. Dorman[25], writing when the so-called "second generation" of OSINT remained in its infancy, talks substantially about software developments that could specifically facilitate the mass collection of open source information. Dorman also takes note, one might argue ahead of his time, of the importance the open source or "free information" movement

[24] Richard A. Best, Jr., and Alfred Cumming, *CRS Report for Congress: Open Source Intelligence (OSINT) Issues for Congress*, Washington: Congressional Research Service (Library of Congress) Report, 2007.
[25] David Dorman, "Open Source Software and the Intellectual Commons", *American Libraries* 33, no. 11 (2002): 51-54.

would play in debates over liberty versus security in the 21st century. Macdonald and Oettinger[26] likewise address the value of investing in technologies to facilitate the mass collection of open source information. Their analysis is specifically useful for scholars of intelligence, as in addition to their discussions on OSINT technologies, they also address new technologies that could facilitate intelligence collection in general and analytical capabilities regarding all major disciplines. They specifically discuss the potential of supercomputers and software as well as satellite imagery and sensory technology.

Nickerson and Sanders[27] address an important subsidiary topic of OSINT: what has been called "jointness." Their work addresses the institutional and legislative history of the concept of interagency cooperation in a government bureaucracy by considering jointness in the United States military. They review and analyze the implications of seminal legislation on the matter, including the IRTPA, as well as the 1986 Goldwater-Nichols Act. Their literature is significant for a scholar of OSINT because their discussion on *military* "jointness", as they authors themselves allude to in the work, could have implications for the IC and its branches actively utilizing the OSINT discipline.

Haynes and Cappa[28] provide another eccentric but notable source of literature on OSINT. They set out in their work to discuss the potential value of "OSINT tools" in conducting risk assessments to prevent cyber-attacks. While their piece provides a number of interesting theoretical takes on the OSINT discipline's use in countering security threats, their work also details the results of a fascinating experiment conducted

[26] Margaret S. MacDonald, and Anthony G. Oettinger, "Information Overload: Managing Intelligence Technologies," *Harvard International Review* 24, no. 3 (2002): 44-48.
[27] Jackson Nickerson, and Ronald Sanders, *Tackling Wicked Government Problems: A Practical Guide for Developing Enterprise Leaders*, Washington: Brookings Institution Press, 2014.
[28] Darren R. Haynes, Francesco Cappa, "Open-Source Intelligence for Risk Assessment," *Business Horizons* 61, no. 5 (2018): 689-697.

by Haynes and Cappa in which OSINT tools were successfully used to profile a target company's network software, hardware, and key IT personnel.

Cuban Missile Crisis Intelligence Literature

The purpose of this final section is to very briefly highlight the important literature used for *reference purposes* in Chapter Seven of the thesis to evaluate the *accuracy* criterion of the quantitative case study. The sources used for the quantitative study itself are all primary sources, but a number of secondary sources were employed to broadly contextualize the crisis and the institutional environment in which the Federal Broadcast Information Service was operating under during the years immediately preceding and shortly following the crisis.

Arguably the two best books on the day-by-day, hour-by-hour progression of the crisis are: Fursenko[29] and Dobbs[30]. These two texts were religiously consulted in the writing of Part Two of this thesis. Both of these works are a necessary read for any scholar or researcher looking to closely examine the intelligence and national-security "fine details" of the crisis. However, the author will dare to qualify that he found greater use in Dobbs's publication than he did in Fursenko's. Fursenko's publication so excessively dwells on the internal politics of Castro's Cuba that doing so largely takes away and distracts the reader interested in the crisis itself from the more relevant details of the international political crisis of 1962.

[29] Aleksander Fursenko, *One Hell of a Gamble: Khrushchev, Castro, and Kennedy, 1958-1964: The Secret History of the Cuban Missile Crisis*, New York: W.W. Norton & Company, 1998.
[30] Michael Dobbs, *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War*, Visalia: Vintage Press, 2009.

On the national security side of the crisis, one must turn to Blight and Welch.[31] The work of these two scholars emphasizes what the authors call the "mundane" issues of the crisis: namely, the many intelligence developments that are critical for any understanding of the crisis and the decisions on all sides that were ultimately made. Blight and Welch also make a case for why scholars of the crisis have devoted more attention to the national security decision-making of the crisis and not enough to the "minor" intelligence details—they cite a paucity of available sources and what they call "natural interests" toward the more "exciting" happenings of the crisis.

Johnson[32] served, in addition to Fursenko and Dobbs, as an essential source on the national security decision-making dimensions of the crisis. While Johnson's work is largely devoted to reexamining "traditional" hypotheses on "victory" and "defeat" during the crisis (and takes the rather controversial stance that the US "victory" was not as complete as scholars, politicians, and the general public alike have tended to agree was the case), the scholar also usefully chronicles and analyzes the major decisions that were made during the crisis that researchers seeking to generally understand the national security decision-making of the crisis would find useful.

Lastly, a source worth mentioning in this literature review for its merit but not an independent scholarly work itself per se is the Foreign Broadcast Information Service's (FBIS) almost completely un-redacted institutional history of its operations during the decade of 1957 to 1967.[33] This over 300-page report provides an invaluable quantity of

[31] James G. Blight, ed., and David A. Welch, ed, *Intelligence and the Cuban Missile Crisis*, New York: Routledge, 1998.
[32] Dominic Johnson, *Failing to Win: Perceptions of Victory and Defeat in International Politics*, Cambridge: Harvard University Press, 2006.
[33] Foreign Broadcast Information Service History Part III: 1957-1967, Washington: The Directorate of Intelligence Historical Series, 1972.

information for a scholar seeking to research how the OSINT discipline was operationally managed during the time period in which this report documents. While this source is only utilized for contextual purposes in this thesis, it is highly recommended that any scholar wishing to better under the Cold War era functioning of OSINT in the IC should aggressively explore this source.

Furthermore, while the source provides a large amount of statistics and organizational facts it should be cautiously approached. As far as I am aware, there is no other record as comprehensive as this FBIS report that chronicles the internal functioning of the US government's major OSINT-capable intelligence organization. Relying on a single source for information is always a danger for any scholar interested in seeking the truth. However, until further FBIS documents and other IC documents are declassified, corroborating this information will be challenging.

This concludes the literature review. With that, the thesis turns now to the first variable of the fundamental relationship in question: Open Source Intelligence.

CHAPTER THREE: OPEN SOURCE INTELLIGENCE

As established, this thesis seeks to consider a relationship between two variables. The first variable can be broadly categorized as *national security decision-making*. The second may be called the *Open Source Intelligence (OSINT) intelligence discipline*. The relationship being considered is how the "raw" and finished products of the OSINT discipline impact the national security decision-making of policymakers and policy outcomes.

In order to understand a relationship between any two variables, one must first consider the defining characteristics of each variable in isolation. Once the variables are adequately defined, only then can one accurately reason or quantitatively test the relationship between the two. The need to define these variables in isolation is especially pertinent when the considered variables encompass broad concepts. Both OSINT and national security decision-making admittedly encompass broad concepts. However, the concepts are not so broad as to be considered beyond categorization. OSINT may at first consideration appear to be narrow concept, but as this chapter will detail, OSINT is a *process* and not an outcome. Indeed, all intelligence disciplines can be characterized as so. The production of a finished OSINT-exclusive intelligence product or a finished all-source intelligence product with OSINT-produced components is the result of an oftentimes-intricate and interrelated sequence of events, ranging from collection of open source information or data to distribution to policymakers. Likewise, national security decision-making is also far from being a monolithic variable. The decisions that policymakers make on questions of national security are motivated by a number of

factors. As the end of this chapter and the chapter that follows will seek to argue, a crucial factor in this particular type of decision-making is the intelligence policymakers receive. The thesis will discuss how intelligence products in general, coming from all disciplines, are a component, and consequently impact, national security decision-making, but will especially focus on how intelligence of the OSINT discipline variety achieves the same effect.

A subsidiary means of understanding a variable is by understanding how that variable impacts other similar but distinct variables. For example, a scientist seeking to deduce how Chemical X will impact Chemical Y may begin her analysis by testing X on Y's relative-chemical, Chemical Z. Likewise, an archer interested in understanding how arrows fly in extreme heat may first consider how an arrow shot in other extreme weather, like extreme cold, affects its aerodynamics. This chapter will utilize similar logic in discussing the OSINT variable.

The chapter begins by deconstructing the first variable: OSINT. It will first define OSINT, review its institutional history and then distinguish the discipline from its sub-component of OSINF. The latter part of the chapter seeks to add to existing literature on OSINT by outlining three novel present and potential uses of the intelligence discipline. In doing so, the deconstructed OSINT variable will be reconstructed and considered in contexts in which it acts independently from the national security decision-making variable. The chapter will conclude by reviewing the above and beginning to establish the framework of open source intelligence's role in the US national security system.

Defining OSINT and OSINT History

The deconstruction of the OSINT variable begins with defining what OSINT is and reviewing its institutional history. The definitional and institutional components that will be pieced apart from the broad concept of OSINT will be elaborated on in more detail as the chapter continues.

There is no universally accepted definition of OSINT, especially within the bureaucratic cobweb of the United States Government. Consider just four definitions of OSINT as defined by scholars and various organizations of the federal government. The Office of the Director of National Intelligence (DNI) defines OSINT as, "[I]ntelligence 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."[34] The United States Army defines OSINT as, "[T]he intelligence discipline that pertains to intelligence produced from publically available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement."[35]Legal scholar Andrew V. Moshirria defines OSINT as: "[T]he systematic collection, processing, analysis and production, classification and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security."[36] The United States Department of Defense defines OSINT as: "Information of potential

[34] Heather J. Williams, and Illana Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, Boston: The RAND Corporation, 2018.
[35] Open-Source Intelligence, Headquarters of the Department of the Army, Washington: 2012.
[36] Andrew V. Moshirnia, "Valuing Speech and Open Source Intelligence in the Face of Judicial Deference," *Harvard National Security Journal* 4, no. 2 (2013): 389.

intelligence value that is available to the general public."[37]

The list could go on indefinitely. How does one define OSINT then? One logical way to do so is by finding definitional commonalities and synthesizing these commonalities from previous definitions. From the four previously sampled definitions, one can identify commonalities. Open Source Intelligence evidently must involve *publicly available information*; a movement of such information through the *intelligence cycle* of collection, processing or exploitation, analysis or production, classification, and dissemination; a cycling of the open source information in a *timely manner*; and lastly, the satisfaction of a particular *intelligence consumer requirement*. Morphing these commonalities into one, new definition, this author posits the following definition for Open Source Intelligence:

> *Open Source Intelligence is the intelligence discipline in which publicly available or legally accessible information is synthesized through the intelligence cycle of collection, exploitation, analysis, classification, and dissemination in order to meet a specific intelligence consumer requirement.*

With this working definition of OSINT established for the thesis henceforth, the remainder of chapter will proceed to take note of a number of terminological nuances in this definition and deconstruct them accordingly.[38]

OSINT as an intelligence discipline is often described as "new" because of its

[37] Donald L. Madill, "Producing Intelligence from Open Sources," *Military Intelligence Professional Bulletin* 34, no. 4 (2005): 19.

[38] Note however that the author will assume the reader is at least partially familiar with the basic terminology of intelligence studies as an academic discipline, regarding terms such as "intelligence cycle" and "collection discipline". For more information on the basics of intelligence studies consult the textbook, Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security*, New York: Columbia University Press, 2007.

primary focus today on publicly available information collected from the Internet and social media. Individuals are making public information available in ways that did not exist or were only in their infancy two decades ago, including through expressions of personal sentiment on blogs and other websites, social media photographs, and publicized social and professional networks.[39] OSINT in many ways is a result of these changes—or the result of a changing human-information relationship in the 21st century.[40] As one observer put it, "…OSINT is taking on a life of its own *outside* [emphasis added] the government."[41]

OSINT may be "new" in this regard, but the history of the discipline extends far before the advent of personal computers, the Internet, and online social media. OSINT's origins date back to the Second World War, primarily as a defense-enterprise.[42] Its institutional history begins in 1941, with the Foreign Broadcast Monitoring Service (FBMS). This wartime organization, operated by the Federal Communications Commission (est. 1934), was established to monitor and analyze the propaganda programs of the Axis powers. It was entirely financed by special defense appropriations. During the war, military intelligence typically turned to OSINT when human and signals intelligence failed. One of the most celebrated World War II cases of this was one incident during the war when the US Air Force was trying to determine if a previous bombing of a bridge outside of Paris had successfully disabled the bridge to all traffic.[43] Military intelligence analysts were unable to confirm if the bridge had indeed been

[39] Williams & Blum, Defining Second Generation Open Source Intelligence (OSINT), 1.
[40] Michael Glassman, and Min Ju Kang, "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)," *Computers in Human Behavior* 28, no. 2 (2012): 673.
[41] Loch K Johnson, ed., *Handbook of Intelligence Studies*, New York: Routledge, 2006, 135.
[42] Williams & Blum, Defining Second Generation Open Source Intelligence (OSINT), 4.
[43] As recounted in Moshirnia, "Valuing Speech and Open Source Intelligence", 391.

sufficiently damaged, so they turned to FBMS analysts for help. FBMS analysts cleverly looked at the price of oranges in Paris to determine if the bridge had indeed been disabled. They deduced that because the bridge was an essential avenue for oranges being transported into the city, if the bridge indeed was hit, then the prices of oranges shortly after the strike in Paris would skyrocket. Sure enough, an inspection of orange prices after the bombing revealed that prices were indeed up significantly. Before aerial reconnaissance confirmed that the bridge was destroyed, FBMS analysts used publicly available information to confirm that fact.

Merely a year after its founding, FBMS would change its name to the Federal Broadcast Information Service (FBIS), a name it would retain for the next 63 years of its existence. When the war ended, FBIS remained under the War Department. Recognizing the vital intelligence role FBMS played during the war, the 1947 National Security Act officially transferred the authority of organization to the Central Intelligence Agency (CIA).

FBIS, by now the OSINT institutional arm of the postwar US Intelligence Community (IC), was a major source of finished intelligence during the Cold War. Defining and refining so-called *First Generation* OSINT, FBIS's purview within the IC until the 1990s was primarily to monitor and translate foreign press service publications available from newspapers, press releases, speech transcripts, and radio and television broadcasts. Especially notable FBIS Cold War accomplishments included providing the first indicators of Soviet removal of missiles from Cuba in 1962[44]; providing early warnings of the Soviet withdrawal from Afghanistan during the Soviet-Afghan War of

[44] Chapter Seven's case study analysis of the Cuban Missile Crisis of 1962 will elaborate more on the Cold War internal operation of FBIS during the crisis.

1979-1989; providing context on the Hungarian Revolution of 1956 and the 1968 Czechoslovakia Uprising; as well as providing approximately 80% of the intelligence used to monitor the collapse of the Soviet Union in the late 1980s through 1991.[45]

When the Cold War ended and the CIA began facing pressure from Congress to reduce its budget, FBIS was considered one potential CIA project to slash funding from for the 1997 fiscal year. Thanks mostly to a public campaign led by the Federation of American Scientists and the IC recognizing that the new 21st century technological landscape would increase the demand for OSINT products, FBIS was preserved. In 2001, as Congress, the public, and the IC itself began assessing the intelligence failures that led to the September 11th terrorist attacks, attention was partially paid to FBIS. In 2004, a report authored by the Office of the Under Secretary of Defense for Intelligence found inconsistences and deficiencies in open source policy and doctrine, training, and management. The report concluded that OSINT under FBIS was at the time largely unchanged from its Cold War function and needed to be adapted to meet the "Information Age" needs of the new millennium. In response to the report, a Defense Open Source Council (DOSC) was created to implement its recommendations. By 2005, with the support of recommendations from DOSC and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, the DNI created a successor organization to FBIS called the Open Source Center.[46] Like FBIS, the OSC was placed under CIA purview, the latter being categorized as the former's "functional manager."[47] The main difference between FBIS and the OSC was that the OSC was tasked with going beyond traditional

[45] Williams & Blum, Defining Second Generation Open Source Intelligence (OSINT), 4.
[46] The IRTPA of 2004 specifically called for the creation of an intelligence center dedicated to "the collection, analysis, production, and dissemination of open-source intelligence [sic]." See ibid., 6.
[47] Ibid., 6.

foreign broadcast monitoring and translation to implementing a system for producing finished OSINT products based on open source information from 21st century technologies like the Internet and social media. The OSC would see another year of bureaucratic reshuffling in 2015 when it was renamed yet again, this time to the Open Source Enterprise and moved under a newly created sub-branch of the CIA called the Directorate for Digital Innovation.

OSINF and OSINT

With the OSINT variable now defined and its institutional history outlined, it is essential, before proceeding, to turn next to distinguishing and deconstructing an implied component of the OSINT definition—that of open source information (OSINF) and how it relates to finished open source intelligence products.

It is crucial to emphasize that OSINF is *not* equivalent to OSINT. OSINF is a type of information. OSINT is an intelligence discipline that ideally results in the production of finished open source intelligence products. OSINF can be defined as, "material that can be lawfully obtained through request, purchase, or observation by a member of the public…[it] includes open-source data but also includes material of more substantive content."[48] Intelligence analysts use OSINF to produce finished OSINT intelligence products for policymakers use (or disuse). A helpful analogy is that OSINF is to OSINT as constructed engine parts are to a functional (or dysfunctional) engine.

Furthermore, OSINF can be subdivided into four major categories: (1.) news media content; (2.) gray literature; (3.) long form social media content; and (4.) short-

[48] Ibid., 10. Note that open source data, at least in this context, includes raw print, broadcasts, oral debriefings, or other forms of information from a primary source. See ibid., 5.

form social media content.[49] News media content includes information from publicly available sources that self-identifies as or is publicly recognized as journalism, such as newspapers, journals, and news aggregator sites. Gray literature is content that comes from non-media institutions and organizations both public and private. Such material includes material from research establishments, national governments, private publishers, and corporations. Long form social media is text heavy social media content from single-individuals or small groups, such as blog posts, Reddit threads, and Tumblr content. Lastly, short-form social media content includes material from social networking platforms such as Facebook, Twitter and LinkedIn. Unlike long-form social media content, short-form social media content tends to have little intelligence value when individual content (i.e. individual Facebook posts or Tweets) are scrutinized. The intelligence value of long-form social media increases when short-form social media, open source information is collected in the aggregate. News media content and gray literature are widely considered to be what OSINT as an intelligence discipline traditionally utilized in its First Generation of existence. The advent of the Internet and online social media created the latter two subdivisions of OSINF, part of the discipline's Second Generation.

Returning to the working definition of OSINT, the discipline is divided into a number of sometimes distinct, and often times interrelated, phases of finished intelligence product production: *collection, exploitation, analysis, classification, and dissemination*. Each of these definitional components can be defined and further deconstructed.[50] The

[49] Categories taken from, Ibid., 11-12.
[50] Moshirnia, "Valuing Speech and Open Source Intelligence", 389-391. Note that the discussion that follows is a discussion of how OSINT in the United States *theoretically* functions. Also note that OSINT, while an independent discipline through FBIS/OSC/OSE, is often a component of all-source intelligence

process begins with *collection*. At this stage, OSINT analysts begin to gather OSINF from all of the previously listed subdivisions of open-source information. Information is acquired from the public domain, unclassified or declassified foreign government documents, books, magazines, newspapers, and scholarly journals, among other sources. Collectors will classify OSINF based on the sensitivity of the sources and the means through which the information was collected. Being publicly available information, collected OSINF is typically unclassified, although depending on the type of OSINF (i.e. grey literature) and the labors involved in collection, OSINF can be classified. Intelligence analysts in general, but particularly analysts of the OSINT discipline, have noted the bureaucratic stovepipes problem associated with over-classification.[51]

Next, analysts then *exploit* or process the aggregate information compiled by collectors.[52] Exploitation is the conversion of OSINF, "raw" intelligence, into a form suitable for analysis and ultimately production of a single finished intelligence product. Exploitation consists of reorganizing and sorting the acquired OSINF. At this stage in the OSINT cycle, information is prepared for the next and most important phase of the process, *analysis*. At this stage, the exploited information is evaluated, integrated, analyzed, and interpreted by one or more intelligence analysts tasked with producing a finished intelligence product, to eventually be distributed to policymakers.[53] It is the job

---

products, which includes finished intelligence from other intelligence disciplines like HUMINT and SIGNINT. One can define the "intelligence cycle" as "…[the] process by which raw data and information are converted into intelligence, through the succession of several phases, which are collection, filtering, processing, analysis and dissemination." See Razvan Grigorescu, "The Role of OSINT In Achieving and Maintaining Security." Paper presented at the International Scientific Conference Strategies XXI: the Complex and Dynamic Nature of the Security Environment, Bucharest, Romania, November 22-23, 2012.

[51] Ibid., 390.

[52] Ibid., 389-391.

[53] Similar to other intelligence disciplines, the analysis phase of the OSINT cycle is typically tiered. The "research paper analogy" may be useful to understanding what is meant by this. The analysis phase of the cycle is in many ways analogous to the manner in which one ideally composes a research paper. The lowest

of the intelligence analyst to act as a kind of detective, identifying patterns and synthesizing and deducing conclusions from an oftentimes-wide range of exploited information. Finished OSINT products will be reviewed for a final *classification* determination after the analysis phase is concluded.

The last stage of the OSINT cycle is *dissemination*.[54] Dissemination is the transfer of finished OSINT products to policymakers. Intelligence is distributed on a "need-to-know" basis. Who "needs to know" is based on constitutional and other legal sources of authority as well as assigned security clearances. The purpose of classification is to ensure that individuals viewing a piece of intelligence do not pose a security risk of exposing the sources and methods used by the IC to produce the finished product. Policymakers have the liberty of doing what they please with finished intelligence products that end up on their desks, including ignoring the products all together.

In summary, OSINF undergoes an often long and multi-faceted journey to becoming a finished OSINT intelligence product. By the dissemination phase of the cycle, the raw information that was obtained during collection typically bears little resemblance to the finished product policymakers receive. Having a basic understanding of the major phases of the OSINT intelligence cycle is necessary in deconstructing OSINT as a variable.

Uses of OSINT

The primary task of the IC is to provide policymakers with timely, accurate, and

---

analysis production tier is the equivalent of writing a "rough" or "first" draft of the finished intelligence product sought. The next tier up edits and further refines the previous "draft", producing a "second" draft. The process continues indeterminately until the highest levels of the IC hierarchy produce a "final draft" or a final finished intelligence product ready for policymaker distribution.

[54] Ibid.

actionable organized and analyzed information they can use to make better-informed decisions. OSINT has proven to be a useful means of fulfilling the IC's primary function. Legendary intelligence community analyst Sherman Kent estimated that in peacetime approximately 80% of information policymakers need to make decisions is available publicly.[55] In recent times the OSINT discipline has been of great use to military policymakers, especially in providing information for counterterrorism operations.[56] In one case, OSINT was able to use Google and other public search engine tools to locate the physical address, fax number, email addresses and even resume of a Hezbollah affiliate living in Africa. In another case OSINT was used to obtain the names of several al-Qaeda cyber actors that were utilizing social networking tools, like Twitter and Facebook, to conduct propaganda and recruitment activities. In a third case, OSINT was utilized to locate several online terrorist nodes, how they communicated, their affiliates, and in some cases even where these cells were physically located.

Despite a number of recorded historical instances in which OSINT proved valuable to policymakers both on the political and military level, intelligence scholars and policymakers remain divided on the *relative* value of OSINT. Generally speaking, three prevailing views regarding the discipline's relative value exist.[57] The first view argues that policymakers derive less value from OSINF than from clandestinely collected secrets. This view is often expressed by those operating with the bias, contrary to what historical evidence suggests, that only secret information has intelligence value. The second view stands in contrast to the first. In this view, OSINF should be seen not only as

[55] Richard A. Best, Jr., and Alfred Cumming, *CRS Report for Congress: Open Source Intelligence (OSINT) Issues for Congress*, Washington: Congressional Research Service (Library of Congress) Report, 2007, 2-3.
[56] Grigorescu, "The Role of OSINT In Achieving and Maintaining Security", 464-65.
[57] Best, Jr. & Cumming, CRS Report for Congress: Open Source Intelligence (OSINT), 2-3.

an important contextual supplement to secret information, but also as a potential source of valuable intelligence, in and of itself. The third and so-called "middle ground" view admits that OSINF will oftentimes never provide "smoking gun" evidence on an issue or threat, but it can, in many instances, be instrumental in helping analysts to better focus or "drive" clandestine collection activities by giving them scope.

Now that the OSINT variable has been deconstructed in both definition and in institution, the variable will now be reconstructed for the purpose of considering contexts in which it acts independently of the national security decision-making variable. By "independently" it is meant considering OSINT as a variable *solely in the intelligence context*. With the subsidiary purpose of defining novel present and potential uses of the discipline, this section will consider the relationship between the OSINT variable and three other potential intelligence variables of interest relating to, but distinct from, the national security decision-making variable: (1.) counterintelligence; (2.) commercial off-the-shelf (COTS) tools; and (3.) all source intelligence and inter-agency integration.

Counterintelligence Potential

Counterintelligence is intelligence gathered about an adversary's intelligence activities and capabilities.[58] Said another way, its purpose is to unmask adversarial intelligence operations and capabilities. While counterintelligence is often thought of and portrayed in television and other media as exclusively human intelligence or HUMINT work—conducted through double agents, spies, and traditional espionage tradecraft—in reality it is often a product of other disciplines as well, including OSINT. It is no secret that late 20th and early 21st century advances in information technology have created new

[58] William E. Odom, *Fixing Intelligence: For a More Secure America*, New Haven: Yale University Press, 2003, 173.

internal data security problems for many companies and large corporations. Cyberattacks pose a threat to organizations seeking to protect the integrity of their data and computerized services essential to their day-to-day operations.[59] OSINT can serve as both as an offensive tool of governments seeking to conduct counterintelligence operations against adversaries and a defensive tool to conduct risk assessments and prevent cyberattacks within their own countries.[60]

Cyberattacks are often caused by IT vulnerabilities, lack of employee awareness, and the social engineering and leveraging of technology and human emotion to gain access to a target system. Websites and social media networks can produce large quantities of personal information and information on behavioral attitudes of individuals and companies that can be of great use to an OSINT agent tasked with counterintelligence. To demonstrate the tactical potential of OSINT counterintelligence, consider the following experiment two researchers—Darren R. Haynes and Francesco Cappa—conducted a year ago.[61]

The experimenters created a hypothetical OSINT counterintelligence assignment for themselves: to profile the IT infrastructure of a specific critical infrastructure company and gather personal information on a key employer. They selected a critical infrastructure company because of the major implications regarding human welfare, the environment, and economic wealth for a modern society such firms generally have embedded in their institutional purpose. By using open sources, the researchers were able

[59] Since the early 2000s, the number of organizations reporting cyberattacks rose to around 50%. By 2011, almost 80% of IT corporate executives reported that their firms had been the target of a cyber attack. Darren R. Haynes, and Francesco Cappa, "Open-Source Intelligence for Risk Assessment", *Business Horizons* 61, no. 5 (2018): 689.
[60] Ibid.
[61] Ibid., 690-693.

to collect precise information on one key IT employee of the firm as well as the IT structure of the firm in general.[62] They utilized several open sources to draw these analytical conclusions: business and social networks, technical job postings, network domains, web-scraping scripts,[63] the Yahoo search tool, the Maltego open source link analysis tool, and a user-scripted tool based on Python. They concluded their study suggesting that exploiting the information collected on the adversarial operating system or the IT employee target could be used to provide information to a policymaker on potential tactical ways to further compromise the operating system with a virus or ways to blackmail the employee through a covert operation.

In summary, considering the OSINT variable exclusively in an intelligence context, there is reason to believe that in increase in OSINT technical capabilities could improve IC counterintelligence operations in the aggregate.

Integration of COTS Tools

OSINT as an intelligence discipline also shows potential for being an effective testing ground for integrating more and new commercial off-the-shelve (COTS) tools into Community collection and analytical apparatuses. The collection and analytical demands of OSINT may influence what types of and how incorporated COTS tools are in the OSINT discipline itself but also the IC as a whole.

On the intelligence discipline spectrum of incorporation of technological tools into the collection discipline, OSINT has traditionally placed more on the "less-technical"

[62] Highlights of their conclusions included the following: (1.) that the company utilized a Windows XP operating system, no longer supported by Microsoft and posing a number of security risks; (2.) that the system utilized two-factor authentication; (3.) identities of coworkers and family members associated with the target IT employee; (4.) personal information on the target IT employee including his hometown, that he has a wife and son and daughter, that he enjoys alcohol, and that he often travels to New York City for Yankees games. See ibid.

[63] That is, a means of harvesting structured data publically available on the Internet.

end, with the discipline of HUMINT, whereas the oft-perceived "technical" disciplines of signals intelligence (SIGINT), measurement and signature intelligence (MASINT), and geospatial intelligence (GEOINT) have been placed on the other end. However, as evidence presented in this chapter and the previous sub-section has suggested, OSINT no longer remains the largely "un-technical" discipline it perhaps was during the heyday of FBIS, pre-1990 (First Generation).

Indeed, elements within the IC utilizing the OSINT discipline employ a wide variety of COTS tools to produce finished intelligence products.[64] IT firms develop most COTS tools for commercial purposes such as advertising, brand management, and consumer analytics, however these tools also have tactical intelligence production value.

To demonstrate this value, consider the two specific program types of existing COTS tools.[65] The first major sub-division is *linguistic COTS tools*.[66] Utilizing these linguistic tools, the analyst might begin with a *lexical analysis*. Such an analysis aggregates large bodies of text from all over the world at a given time from multiple sources and languages to look for trends in syntax. If the analyst is more interested in diction than syntax, a *keyness analysis* could be conducted instead. A keyness analysis aggregates data on individual words such as how often certain words appear in writing from a given source or sources. A diction analysis alternative might be a tool that analyzes clusters instead. Clusters are a sequence of two or more words that may not be grammatical or meaningful by themselves, but to the contextual needs of an analyst may

[64] Williams & Blum, Defining Second Generation Open Source Intelligence (OSINT), 21.
[65] Note that the tools listed in this paragraph are examples likely to be used with long-form social media content and short-form social media content of OSINF. Ibid., 23-35.
[66] A term invented by this author. The second sub-divisionary term used in the following paragraph, "content-based COTS tools", was also invented by this author. The terms that follow in each paragraph were developed by Williams & Blum. See ibid.

be indicative of a greater importance. If the analyst seeks more of a comparative tool then he or she may turn to a *frequency profile*—a program that allows the user to compare one textual corpus to another based on the occurrence of keywords in each body.

The second major subdivision of COTS tools is *content-based COTS tools*.[67] Whereas linguistic COTS tools are designed to break down the textual bodies of social media OSINF, based on structural considerations like syntax and diction, content-based COTS tools use machine learning to aggregate data and analyze information based on topics, themes, and substantive issues found within a data set.[68] Two examples of content-based COTS tools are *sentiment analysis* and *stance analysis*. In sentiment analysis, a program identifies terms of entities about which a person has an overall majority opinion not shared by a different class. An example might be the opinion of a "fringe" figure like a terrorist, compared to the opinion of say the average working-class citizen of a country. A *stance analysis* on the other hand focuses less on feelings and more on established principles. Stance analyses use language preferences to indicate an individual's underlying values or an expression of their attitude toward a given concept. In one study utilizing a stance analysis program, the researcher, in analyzing a variety of social media communications by members of the US Marine Corps, was able to conclude that Marines speak in a distinct, internally cohesive manner, "marked by future-oriented, inclusive, [and] highly certain language."[69]

The further development, emergence, and use of COTS tools in OSINT can be

[67] Ibid.
[68] "Machine learning" can be defined as the process of teaching a software program to make decisions independent of a human after the desired decision making process has first been modeled extensively for the program. See Alex Hern, "Google says machine learning is the future. So I tried it myself", *The Guardian*, June 28, 2016.
[69] Researcher William Marcellino conducted this study. See ibid., 26.

characterized as the "future" of the intelligence discipline. The greater the incorporation of these analytical tools into OSINT, the more likely OSINT will be able to further distinguish itself from other intelligence disciplines as well as ultimately increase the analytical depth to its work. COTS tools encompass the fabric of what has been more widely called the "open source movement" or the "open source software method."[70] With new developments and capabilities in information technology, the legal and economic status of information is changing rapidly. Questions relating to who will control access to information, how society will coordinate and manage the flood of digital information, how the Internet will be filtered and by whom, as well as copyright issues, and information literacy, define the scope of the open source movement. Open source software seeks to extend the intellectual commons into the realm of computer software in an effort to prevent the tight control of information content from being in the exclusive hands of its private sector software developers. One of these potential mediums to "liberate" this software could involve a greater implementation of COTS tools into the fabric of the IC—particularly in the realm of OSINT, through acquisition of such tools from the private sector, but more importantly, through Community funded initiatives to research and develop tools of their own to meet their specific collection and analysis requirements. If the "information revolution" has provided the other intelligence disciplines of the IC and its customers with supercomputers, high resolution satellite imagery, sensors that penetrate natural and manmade barriers, and software for information processing, it is improbable that further developments in COTS tools would

[70] David Dorman, "Open Source Software and the Intellectual Commons", *American Libraries* 33, no. 11 (2002): 51.

not also likely be incorporated into the OSINT fabric.[71]

All-Source Intelligence and Interagency Integration

Lastly, there is reason to believe that the OSINT variable seen exclusively in an intelligence context improves the quality of all-source intelligence[72] and serves as an impetus to fostering interagency integration within the IC.

OSINT has uses beyond the production of its own discipline-exclusive finished intelligence products for policymakers. In fact, OSINT is likely to prove to be increasingly needed to integrate OSINF into finished, all-source intelligence products. Advocates for greater attention to the value of OSINT in the IC do not exclusively point to the need for a greater number of open source practitioners. They also note agency cultures as an area of concern—namely, that such cultures need to change so that the use of open source information is a more "routine" and "natural" component of analytical practice.[73] It is no secret that to this-day many scholars, policymakers, and analysts alike devalue OSINF by virtue of its "publically available" nature. The cognitive bias that for the intelligence analyst, information is only valuable if it is secret unfortunately remains pervasive.[74]

---

[71] Margaret S. MacDonald, and Anthony G. Oettinger, "Information Overload: Managing Intelligence Technologies," *Harvard International Review* 24, no. 3 (2002): 44.

[72] All-source intelligence is, "the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence." See "Part Three: Military Intelligence Disciplines," *Global Security*, https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap5.htm (accessed January 30, 2019). Note that all-source intelligence is a separate intelligence discipline—despite producing finished intelligence products that aggregately collect information from the other disciplines—as well as the name of the act of using "all-sources" to produce intelligence from multiple intelligence sources.

[73] Richard A. Best, Jr., and Alfred Cumming, CRS Report for Congress: Open Source Intelligence (OSINT), 13.

[74] Loch K Johnson, *Handbook of Intelligence Studies*, 134. Johnson writes, "It is a common misperception that most 'intelligence' is classified and must come from secret sources and methods that are very expensive and relatively risky. The 'cult of secrecy' has put us in a very disadvantageous position, where in the United States of America…at least $50 billion a year is spent on collecting the 5% of the information

The end of the Cold War and the need to adapt IC practices to a new, 21st century world led to the publication of several government reports recommending more effective incorporation of OSINF into Community-produced, all-source finished intelligence products. The following is a brief summary of the major reports that were published on this matter.

The first major report, conducted by the 1995-96 Aspin-Brown Commission, concluded that the IC needed to make greater use of OSINF in the millennium ahead, stating that the IC of the later 1980s and early 1990s had only limited access to open source databases in its day-to-day operations. Furthermore, the report sustained that adopting less "intrusive" security measures could be one means of internally opening the IC to more efficient collection and use of OSINF.

The next major report was published following the September 11th terrorist attacks, the 9/11 Commission Report.[75] While extensively discussing the failures of the IC to take preventative actions to foresee the attacks in New York and elsewhere, it only makes very brief mention of open sources at the very end of the report, referencing the need for the creation of an "Open Source" center within the Central Intelligence Agency.[76] The report does not go into any more detail on how such a center would be organized.

A year later another report would be published, building off of the vague OSINT vision of the 9/11 Commission Report and reiterating nearly a decade latter the message

---

that is secret and can or must be stolen, and virtually nothing is spent on the 95% of the information in all languages that is relevant to all but the most sensitive threats."

[75] Loch K. Johnson, "The Aspin Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission," *Central Intelligence Agency Library* (Washington, D.C.), April 14, 2007.

[76] A simple "Command + F" shortcut search on a PDF of the entire report reveals that the words "open source" make only a single appearance in the document. This appearance is in a diagram recommending how to restructure the IC in the aftermath of 9/11. Kean, Thomas H., et al., The 9/11 Commission Report, Washington: The 9/11 Commission Members & Staff, 2004, 413.

of the Aspin-Brown Report. The 2005 Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (often abbreviated, "the WMD Commission" or "the WMD Commission Report") concluded that the IC continues to make too little systematic use of outside experts and OSINF in its day-to-day operations.[77] The report added that while it recognized the IC value of concentrating on readily available, "secret" material in producing intelligence assessments, it also urged policymakers and other readers not to undervalue OSINT's potential value.

The Open Source Center vision would be actualized in 2005 thanks to the advice of all three of these reports. However, a seminal piece of legislation also motivated the creation of the National Open Source Center.[78] This legislation was the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)[79], which made the most extensive changes to the structure of the United States Intelligence Community since the passing of the 1947 National Security Act.[80]

The two most relevant sections of IRTPA for this discussion are 1016 and 1052, which discuss information sharing and OSINT respectively. Section 1016—while exclusively focusing on the national security threat of international terrorism—calls for the official creation of an Information Sharing Environment (ISE). The ISE is vaguely defined as an "approach" that facilitates the sharing of information on terrorist activities.

---

[77] Laurence H. Silberman, et al., Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Washington: Members & Staff of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005.
[78] Richard A. Best, Jr., and Alfred Cumming, CRS Report for Congress: Open Source Intelligence (OSINT), 11.
[79] Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, *U.S. Statues at Large* 118 (2004): 3638.
[80] National Security Act of 1947, Public Law 80-253, *U.S. Statues at Large* 61 (1947): 495.

"Terrorist Information" is defined as the aggregate information collected, produced, or distributed on factors such as the organization, capabilities, plans or intentions, threats posed, and communications of individual terrorists and terrorist networks against individual Americans and the United States. Section 1052 on the other hand, like the 9/11 Commission Report and also the WMD Commission Report, calls for the establishment of an Open Source Center. Section 1052 of IRTPA is more significant in its call for such a center, because it explicitly grants authority to establish the organizations to the DNI and provides more detail as to what exactly the center will be tasked with achieving. Section 1052 calls for the DNI to establish an intelligence center for the purpose of "coordinating the collection, analysis, production, and dissemination of open-source intelligence [sic] to elements of the intelligence community".[81] Furthermore, the section reiterates the value of OSINF and calls for its further integration into the "intelligence cycle" so as to ensure that all elements of the intelligence community make use of it.[82]

The purpose of detailing this legislative history was to emphasize that policymakers saw and see great importance in expanding the role of OSINT beyond it being its own exclusive intelligence discipline. OSINT shows great potential in the realm of interagency intelligence collaboration.

Understanding the value of interagency intelligence integration and its relation to OSINT requires an understanding of the concept of "jointness".[83] In any bureaucracy—be it governmental or of an intelligence community—the problem of

[81] The section tasks the DNI with producing a report to determine whether or not to recommend the establishment of an open source center. Although the DNI did indeed eventually recommend the establishment of an open source center to both congressional intelligence committees, it is worth noting that the statute does not establish the center *per se*, but rather calls on the DNI to make the determination himself. Public Law 108-458, §1052, (a)(1).
[82] Ibid., (a)(2-3).
[83] Nickerson, Jackson, and Ronald Sanders, *Tackling Wicked Government Problems: A Practical Guide for Developing Enterprise Leaders*, Washington: Brookings Institution Press, 2014.

bureaucratic stovepipes tends to be pertinent. As the post-9/11 IC realized, the stovepipe problem was and is a serious issue within the United States IC. For this reason, key reports like the 9/11 Commission Report and the WMD Commission Report recommended that the IC take actions to better achieve an "interagency" internal unity of effort in the future.

The IC has been encouraged to turn to the US Armed Forces for a model of "jointness" that could be used to better create interagency unity. Military historians and political scientists trace the recent origins of the concept of jointness back to the 1986 Goldwater-Nichols Department of Defense Reorganization Act.[84] One of the major provisions of this act of Congress required that as a prerequisite to flag rank[85], officers in the nation's armed forces would need to complete one or more joint assignments in the inter-service combatant commands.[86] The concept of combatant commands was specifically designed for purposes of integration of the armed services through the concept of "joint duty". The idea behind requiring joint duty was that requiring officers to partake in terms of service in the other branches of the military would provide needed exposure to the bureaucratic and logistical functioning of the commands of these branches. The degree of tactical cooperation required among branches of any 21st century modern military to successfully conduct operations and combat and deter threats is

[84] Goldwater-Nichols Department of Defense Reorganization Act of 1986, Public Law 99-433, *U.S. Statutes at Large* 100 (1985): 992.
[85] That is, the rank in the US armed forces applied to all general officers authorized to fly their own command flags. In the Army, for example, this would include officers of the brigadier general rank or higher. Offenhauer, Priscilla, General and Flag Officer Authorizations for the Active and Reserve Components: A Comparative and Historical Analysis, Washington: Federal Research Division of the Library of Congress Report, 2007.
[86] Established by, Title 10, U.S. Code §161-168. The ten current combatant commands include: Africa Command, Central Command, Cyber Command, European Command, Indo-Pacific Command, Northern Command, Southern Command, Special Operations Command, Strategic Command, and Transportation Command. See "Combatant Commands," United States Department of Defense, https://www.defense.gov/Know-Your-Military/Combatant-Commands/ (accessed December 29, 2018).

unprecedented in the history of warfare, due to the technological complexities that define warfare today.

It is evident that institutionally speaking, policymakers envision the full implementation of a similar system of joint duty in the IC.[87] IRTPA was the first major piece of legislation to call for the creation of such a system[88], to be organized and defined by the Director of National Intelligence. Quoting the section that defines the jointness vision for the IC, in full, is apt:

> "(3) (A) The Director of National Intelligence shall prescribe, in consultation with the heads of other agencies or elements of the intelligence community [sic], and the heads of their respective departments, personnel policies and programs applicable to the intelligence community that—
>
> (i) encourage and facilitate assignments and details of personnel to national intelligence centers, and between elements of the intelligence community;
>
> (ii) set standards for education, training, and career development of personnel of the intelligence community;
>
> (iii) encourage and facilitate the recruitment and retention by the intelligence community of highly qualified individuals for the effective conduct of intelligence activities;
>
> (iv) ensure that the personnel of the intelligence community are sufficiently diverse for purposes of the collection and analysis of intelligence through the recruitment and training of women, minorities, and individuals with diverse ethnic, cultural, and linguistic backgrounds;

[87] Nickerson & Sanders, *Tackling Wicked Government Problems*, 122.
[88] On the question of how a joint system would function, Nickerson & Sanders recommend that joint duty selections not be based on the ad hoc system by which the IC presently fills general vacancies, but instead as the National Counterterrorism Center does by establishing annual aggregate staffing quotas with each individual hiring agency designating contributing staff. See Ibid., 139.

(v) make service in more than one element of the intelligence community a condition of promotion to such positions within the intelligence community as the Director shall specify; and

(vi) ensure the effective management of intelligence community personnel who are responsible for intelligence-community wide matters"[89]

As the legislation makes clear, IRTPA encourages a wide range of jointness initiatives in the IC, including joint-personnel duty assignments; uniform standards for education, training, and career development; and joint-duty as a promotion requirement for "certain positions".

While IRTPA's push for jointness is indeed desirable[90] and in theory effective, the IC's present efforts to implement joint duty initiatives could be improved regarding OSINT inclusion. The existing joint duty apparatus consists of regular joint duty rotations (Civilian Joint Duty Program)[91] and a Joint Duty Swap.[92] The only major difference between the two regards recruitment—that with the latter, no office is left with a vacant position. In neither of these programs is there specific direction on how jointness will be promoted through Community incorporation, implementation, and training regarding OSINT methodology.

The IC faces a range of institutional challenges in altering its general tendency toward keeping the historical agencies of the IC operating independently. The creation of

[89] Public Law 108-458, §102, (3)(A).
[90] The intelligence scholar Roger Hilsman Jr. has stated why this is so simply but correctly: "First hand experience [in another agency] is valuable in many ways—a man who has absorbed everything available on a given subject [in his agency] with a minimum of first-hand experience may still have much to learn [from the other agency]". Roger Hilsman Jr, "Intelligence and Policy Making in Foreign Affairs," *World Politics* 5, no. 1 (1952): 17.
[91] Intelligence Community Civilian Joint Duty Program, Washington: Office of the Director of National Intelligence, 2013.
[92] Intelligence Community Joint Duty DoD Swap Pilot: Many Perspectives One Community, Washington, Defense Civilian Intelligence Personnel System, 2006.

the DNI position and the National Security Council and outlining jointness recommendations in IRTPA are only the beginning of the process of truly making the IC into a cohesive entity it needs to be to effectively face the intelligence challenges of the 21st century world. OSINT remains only a piece of the puzzle that is interagency integration, but as with the other collection disciplines and IC agencies out there, an essential piece if the puzzle is to be completed.[93]

Indeed, there is reason to believe that OSINT may serve as a means of facilitating this desired greater interagency integration, inevitably leading to better all-source intelligence products. It is the fundamental nature of open source information that may serve as the glue. From the less technical disciplines like HUMINT to the more technical disciplines like MASINT, a common font of open source information may better serve the collection and analytical needs of other disciplines. The unity achieved by drawing from the same well of information has tremendous potential to keep the various agencies of the IC "talking." OSINT does not need to be under the purview of one arm of the IC in order to be effective. In fact, all agencies of the IC could find value in the universal applicability of information from open sources.

The Future of OSINT: a Third Generation?

Before concluding this chapter, which has just attempted to reason the operation of the OSINT variable in an exclusively intelligence context, a brief return to deconstructing the variable is in order. However, this return to deconstruction seeks in

[93] For a discussion on the historical origins of operational jointness in the US IC, as inspired by the United Kingdom's Joint Intelligence Committee (est. 1936), see Richard J. Aldrich, et al, *Spying on the World: The Declassified Documents of the Joint Intelligence Committee, 1936-2013*, Edinburgh: Edinburgh University Press, 2014.

part to speculate on the future of the variable—or as the discipline evolves with politics and technological change, to ask how the basic building blocks of the variable may change with time.

One may define two pre-existing "generations" of OSINT.[94] *First Generation* (G1) OSINT was the OSINT of FBIS. Build primarily on translation expertise, G1 OSINT often required "physical" access to OSINF sources—i.e., analysts directly listening to radio broadcasts, watching televised speeches, reading foreign newspapers, etc. Constrained by the technological limitations of the mid-20th century, reports were produced by analysts and eventually disseminated by the top tier of the IC chain of command to policymakers absent advanced computer programs, COTS tools, and even the "simple luxury" of basic word processing programs. Despite these technological limitations, intelligence was more often than not produced in a timely manner and, as explained previously, had a remarkable record of contributing both indirectly and directly to intelligence successes.

The 2005 creation of the Open Source Center (OSC) marked the emergence of a *Second Generation* (2G) variety of OSINT.[95] 2G OSINT distinguishes itself from 1G OSINT for its incorporation of the emerging Internet-computer based technologies of the later 1990s and the first decade of the 21st century, namely social media. 2G OSINT is built on technical expertise as opposed to translational expertise. Where 1G OSINT required physical access to OSINF, 2G OSINT can access most, if not all, OSINF for the

[94] Generations as defined by, Williams & Blum, Defining Second Generation Open Source Intelligence (OSINT), 40.
[95] The period of 2003-2006 is considered to be the "golden age" of the founding of what are today considered to be many of the most prominent social media networks: Myspace (2003), Skype (2003), Facebook (2004), Flickr (2004), Reddit (2005), YouTube (2005), and Twitter (2006). See José van Dijck, *The Culture of Connectivity: A Critical History of Social Media*, New York: Oxford University Press, 2013.

intelligence requirement in question via virtual accessibility. Whereas the 1G OSINT cycle regularly published hard-copy intelligence publications for policymaker use, 2G OSINT, in sharing this characteristic, adds the additional characteristic of constant acquisition of OSINF. 1G OSINT analysts, being human beings, have work and productivity limitations. A computer program constantly collecting OSINF can be operationally active as long as the computer technology it is running on continues to technically function. This technological difference between 1G and 2G OSINT leads to a final point on the latter: whereas the crux of the 1G OSINT is in the analytical and dissemination phases of the OSINT cycle, 2G OSINT's greatest operational potential appears to be in the exploitation and production phase of the OSINT cycle.

In addressing the question of what can be defined as the "future" of OSINT, one must turn to a speculative construction of what *Third Generation* (3G) OSINT could come to constitute. Such a question revolves around the conception of a so-called *Web 3.0*, that is, a "Semantic Web" consisting of direct and indirect machine processing of data, machine-learning, and automated reasoning.[96] G3 OSINT would likely see a more advanced implementation of COTS tools in the process of transforming OSINF into finished intelligence products. More specifically OSINF, when processed with tools based on social network analysis, provides new opportunities for analysts to extend the time horizons of their analysis more into to the future, increasing the likelihood to which they can potentially identify security threats posed by individuals and other targets of interest.[97] G3 OSINT could, and is likely to, go beyond the present OSINT technical capabilities of the present day. It will likely be constructed entirely on machine learning

[96] Williams & Blum, Defining Second Generation Open Source Intelligence (OSINT), 39.
[97] Christopher J. Rhodes, *The Use of Open Source Intelligence in the Construction of Covert Social Networks*, Vienna: Springer, 2011.

and automated reasoning, constructs that previously defined the outer bounds of science fiction but today are a serious technological prospect. Augmented reality is one example: cooperating with HUMINT, such implementation of a "digital layer" of "wearable technology" could have potential for targeting and recruiting of human intelligence assets.[98] Likewise, the data-driven sub-branch of psychology of psychometrics could also be a component of future IC collection endeavors—although some think such incorporation could excessively blur the line between OSINT and psychological information operations.[99]

Conclusion: from OSINT to national security decision-making

To review, this chapter has sought to deconstruct OSINT as a variable terminologically, through its institutional history, and through potential future changes to the discipline as technological capabilities improve. The chapter also considered the OSINT variable, in its monolithic form, in outlining three novel present and potential uses of the OSINT outside of the national security-decision making variable context, exclusively in an intelligence context. A more detailed consideration of what this chapter has substantially concluded is reserved for Chapter Five, when the theoretical nexus (or lack thereof) between intelligence and national security decision-making will be defined in full.

---

[98] The most accessible sources of augmented reality today include *Google Glass* and some smartphone gaming applications like Niantic's *Pokémon Go*. Williams & Blum, Defining Second Generation Open Source Intelligence (OSINT), 40.

[99] An example of the OSINT potential of incorporating psychometrics into OSINF gathering is Cambridge Analytica's data campaign modeling and targeting voters in the 2016 US presidential election. For two views expressing concerns over the implications of using psychometrics in the OSINT intelligence discipline see Ellen Broad, "Are Cambridge Analytica's insights even that insightful?", *The Guardian* (London, UK), March 22, 2018, and Issie Lapowsky, "The man who saw the dangers of Cambridge Analytica", *Wired* (London, UK), June 19, 2018.

The next chapter, dedicated to considering the second variable: national security decision-making, will proceed somewhat differently than the chapter now concluding. Whereas this chapter's sole purpose was to exclusively deconstruct and independently analyze the OSINT variable, the next chapter will begin to build upon what has been presently achieved *in addition to* deconstructing and independently analyzing the second variable. That is, the following chapter will begin to conceptualize why intelligence is a part of the complex apparatus that is the US national security decision-making system. The next chapter will make the case that national security decision-making occurs at the intersection of *formal* structures and institutions and *informal* structures and processes.

CHAPTER FOUR: NATIONAL SECURITY DECISION MAKING

The thesis now turns to independently considering the second variable: *national security decision-making*. Although Chapter Five will explicitly deal with the nexus (or lack thereof) between the two variables, Chapter Four will begin to build off of the variable already established, in an attempt to begin bringing the reader closer to a comprehensive understanding of the relationship (or lack of) between the two.

The structure of this chapter will be as follows: (1.) a history of how the traditional "security" needs of the state transformed into a novel conception of "national security"; (2.) a deconstruction of the national security decision-making variable into its formal and informal components; and (3.) the presentation of a final perspective on national security decision-making, to be applied in Chapter Five with what has been previously established in the chapter on OSINT.

A History: from 'Security' to 'National Security'

The chapter begins with a spattering of history, because understanding national security decision-making is largely a matter of understanding the formal and informal histories of what today can be called "the national security system" of the United States.

Security is a necessity of any functional, non-anarchic society. Without security, people cannot trust their government or their neighbors, nor can they focus on goals extending beyond survival, due to immediate fears such as providing for their families or preparing adequately for the future.[100] One can consider security from many different

[100] Cynthia Watson, *US National Security: A Reference Handbook, Second Edition*, Santa Barbara: ABC-CLIO, 2008, 2.

societal levels: from the personal security needs of an individual or family to the larger security needs of a country or continent. This thesis seeks to consider security from one of its least magnified levels—that of the country or, in particular, the security of the United States of America.

While the word "security" itself appears only one time in the United States Constitution,[101] the preamble of the document establishes that to "provide for the common defence [sic]" and to "secure the Blessings of Liberty" are two of the reasons for establishing a constitution in the first place.[102] The document further elucidates that the executive branch of government under the authority of the president, as established under Article II, will be vested with the authority to command US armed forces.[103] However, executive authority over decisions relating to providing for the common defence and securing liberty are not exclusively under presidential-executive discretion. Article I, in establishing a congress, reserves some of these powers for the legislative branch of government.[104]

Since the beginning of the Republic, security was perceived as having both a domestic and foreign component.[105] Traditional duties of the federal government were very limited in scope: handling mail, regulating immigration, collecting tariffs, and enforcing Prohibition, to name some. The size and purview of the federal government

[101] The Second Amendment reads: "A well regulated Militia, being necessary to the *security* [emphasis added] of a free State, the right of the people to keep and bear Arms, shall not be infringed." See U.S. Const. amend. II.
[102] U.S. Const., Preamble.
[103] "The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States." Ibid., Art. II, Sec. 2(1).
[104] To provide three examples: "The Congress shall have Power To…provide for the common Defence" See ibid., Art. I, Sec. 8 (1); "[Congress shall have the power to] …declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water." See ibid., Art. I, Sec. 8 (11); and "[Congress shall have the power to] …raise and support Armies." See Art. I, Sec. 8 (12).
[105] David Jablonsky, et al., *U.S. National Security: Beyond the Cold War*, Carlisle: U.S. Army War College Strategic Studies Institute Press, 1997, 1-6.

expanded during times of war and times of crisis.[106] During the Great Depression for example, President Franklin Roosevelt's New Deal drastically increased the role of the federal government in affecting the everyday lives of ordinary Americans—through farmer subsidies, market regulation, labor dispute mediation, and aid to the aged and infirm.

Thus, prior to the end of the Second World War, the concept of the federal government implementing "security" policy was limited almost exclusively to the vague prescriptions of executive and legislative branch powers as delineated by the Constitution, except during times of war or national crisis when the government was widely seen as having greater leeway to broaden its powers. Throughout the 19th and early 20th centuries, security questions almost exclusively revolved around territorial sovereignty concerns and questions of neutrality in European-centered conflicts.[107] A combination of the rapid growth of the "wartime bureaucracies" of the United States leading up to and during the war, the US emerging as one of two bipolar powers in the postwar era, and an increasingly globalized economy[108] led to the birth of a new, revolutionary conception of security in the United States: "national" security.

"National security" entered into the government and political lexicon of the United States through the National Security Act of 1947. The purpose of the legislation was:

---

[106] Ibid., "[The US Constitution created]…a weak central government, Cincinnatian in form, expanding in wartime and contracting after every conflict."
[107] Only some of the most prominent historical examples of this included: how to respond to British practices against American shipping during the Napoleonic Wars; whether or not to annex Texas upon its declaration of independence; how to respond to the sinking of the *Maine* shortly preceding the War of 1898; and how to respond to German unrestricted submarine warfare preceding World War I.
[108] Linda Weiss, *The National Security State and Technology Leadership*, Ithaca: Cornell University Press, 2014, 1-2.

> "To promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with national security."[109]

Furthermore, the act created a National Security Council (NSC); unified the branches of the World War II-era military into a single Department of Defense (DoD); and unified the wartime intelligence agencies into a compact Central Intelligence Agency (CIA). The act also implicitly established three major pillars to national security: *national interests*, *security, and grand strategy.*[110] The three concepts are interrelated, but national interests serve as the bedrock. The new conception of security in the post-World War II era has largely been a question of serving those interests.

Formal Structures: The Example of the National Security Council

With the history of how "security" became "national security" now established, this chapter transitions next to deconstructing the second variable of the fundamental relationship the thesis as a whole seeks to consider. This deconstruction begins by piecing aside the first major constituent component[111] of the national security decision-making variable: formal structures of decision-making. While the formal structures of national security decision-making have evolved overtime with different presidential administrations, a number of historical and institutional commonalities shared in every

[109] Public Law 253-343 of July 26, 1947.
[110] For more on what these pillars entail see Jablonsky, et al., *U.S. National Security: Beyond the Cold War*, 1-6.
[111] As a reminder, this chapter seeks to broadly argue that national security decision-making occurs at the intersection of formal structures and institutions and informal structures and processes.

iteration of the formal structures of decision-making have given these formal structures a consistent identity. The purpose of this section is to deconstruct that identity and also establish that intelligence is embedded into the formal structures of decision-making. The institutional mechanisms in place at any given time in the national security system play an important role in policymaker receptivity to strategic intelligence.

The *formal structures* of national security decision-making consist of the bodies established by statute and other structured components of the federal government to procedurally organize and handle decision-making relating to national security. Today, most national-security decision-making passes through the National Security Council. Although other quasi-independent components of the NSC have a degree of national security decision-making authority in their own right—like the various departments of the federal government—ultimately all of these individual components fall under the purview of the NSC.[112] For this reason, this section of the thesis will refer to the existence of "formal structures" in monolithic reference to the NSC, although it is important not to confuse parts to the whole when discussing national security decision-making formal structures in general.

The statutory membership of the National Security Council has changed over

[112] The idea behind what would become the national security formal structure plan of the National Security Act of 1947 was largely inspired by the 1945 Eberstadt Report, drafted by the Task Force on National Security Organization, chaired by Ferdinand Eberstadt. The report is credited for devising the idea of a national security council. The council was intended to concentrate exclusively on foreign and military matters while a National Security Resource Board (NSRB) would focus exclusively on domestic and economic considerations. The NSA of 1947 did indeed create a NSRB, but the organization would be dissolved and its range of activities absorbed by the Eisenhower era NSC less than a decade later. The rival of the Eberstadt Plan, the so-called Collins Plan, divided the upper tier of national security decision making among a body of assistant secretaries, general secretaries, and a chiefs of staff division. The Collins plan was ultimately scrapped when Congress found the Eberstadt plan more desirable. See Robert L Jr Pfaltzgraff, and Uri Ra'anan, *National Security Policy: The Decision-making Process*, Hamden: Archon Books, 1984, 177-180.

time, but it has always been chaired by the President of the United States.[113] Other statutory and non-statutory regular attendees include the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, and the Assistant to the President for National Security Affairs.[114] The Council also has historically sought advise from the Director of National Intelligence (formerly the Director of Central Intelligence)—largely ensuring that the input of the IC is institutionally embedded into the structure. The act gives the president, who is to preside over the Council, a flexible degree of authority to appoint other cabinet and sub-cabinet officials.

The purpose of the Council is to "advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security."[115] This advising has traditionally consisted of six major functions[116]: (1.) routine staff support and information (e.g. speech preparation, trip planning); (2.) crisis management (e.g. handling of the 1962 Cuban Missile Crisis); (3.) policy development (e.g. strategic planning, decision catalyzing, decision management); (4.) policy implementation (e.g. monitoring operations, assessing results, recording and promulgating decisions); (5.) policy advise (i.e. traditionally from the National Security Adviser[117]); and (6) conducting operations (e.g. secret diplomatic initiatives, reception of high level foreign visitors).

---

[113] Lord, *The Presidency and the Management of National Security*, New York: Free Press, 1988, 61-68, 115-146.
[114] "National Security Council," Washington: Executive Office of the President of the United States, 2019.
[115] Public Law 253-343, §101 (a).
[116] Adapted from Carnes Lord, *The Presidency and the Management of National Security*, 61-68, 115-146.
[117] For a superb history of the role of the National Security Adviser and the evolution of the NSC from its Truman Administration birth to the Obama Administration, see John P. Burke, *Honest Broker?: The National Security Advisor and Presidential Decision Making*, College Station: Texas A&M University Press, 2009.

Structurally speaking, the NSC has traditionally had three tiers of organization.[118] At the top tier is the President of the United States, usually advised directly by a trusted inner circle.[119] The president theoretically has the final say in all strategic and tactical national security decision-making choices. While his trusted inner circle and other advisers of the lower tiers of the structured system often inform a president's decisions, as long as the president is acting within his constitutional authority, he is permitted to make final decisions on all national security decision making matters.

Below the presidential level, is the National Security Council itself, which can be further subdivided today into its two major committees: *Principals* and *Deputies*.[120] At the combined level of both committees typically all cabinet level members, including the president, as well as the vice president, participate. However, on the separated committee level, the president and vice president typically do not participate. In the Principals committee, cabinet level membership along with the Assistant for National Security Affairs (ANSA) or "National Security Adviser", as well as his executive secretary and secretariat, take charge. The Principals committee serves a kind-of "quality control" function, often meeting informally shortly prior to a collective NSC meeting with Deputies. The Deputies committee is more expansive than Principals, consisting of subcabinet level membership, often including deputy heads of departments and agencies

[118] Robert D. Worley, *Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System*, Lincoln: University of Nebraska Press, 2015, 352.
[119] Famous historical examples of advisers that have an especially intimate professional relationship with a president include Henry Kissinger (National Security Adviser to President Nixon), Zbigniew Brzezinksi (National Security Adviser to President Carter), and Robert "Bobby" Kennedy (brother and Attorney General to President Kennedy).
[120] Worley, *Orchestrating the Instruments of Power*, 352. Note that the NSC Principals and Deputies committees only date back to the George H.W. Bush Administration. Administrations prior to Bush I had different NSC committee structures. For a comprehensive history of the structural evolution of the national security system see History of the National Security Council: 1947-1997, Washington: Office of the Historian, 1997.

as well as undersecretaries. Deputies meet more frequently than Principals and also have the important responsibility of organizing the next and final tier of the NSC-system: staffers organized in working groups.

In order to effectively advise the president, the Council has traditionally relied on a NSC staff, providing seven important functions for the upper tiers of NSC leadership. These staff members have typically been organized into working groups.[121] Chaired at the assistant secretary level, staff members are ideally nonpolitical experts on the topics their working groups address. They are tasked with providing substantial reports to Deputies and Principals on the tasks they are assigned to research..

The "substantial" tasks staff members at the working group level face can be subdivided into seven different areas. The purpose of providing context on each of these seven functions is to emphasize how intelligence is embedded into the formal structures of national security decision-making and to emphasize the significant *policy formation* and *policy evaluation* roles staffers play in the government at large.

First, NSC staffers have an important role in planning for the NSC. Planning includes reviewing strategic intelligence; making net policy assessments; reviewing long-range strategic planning options; managing short-range and crisis-related tactical options; organizing economic and resource management; and speechwriting.

Second, NSC staffers have a degree of latitude in handling political affairs. Like the organization of the State Department, the organization of NSC is ordered regionally and by country. Take as an example the staffer organization of the 2000 NSC during the

[121] Also adapted from Carnes Lord, *The Presidency and the Management of National Security*, 61-68, 115-146.

Clinton-Bush II pre-9/11 transitional years.[122] During this iteration of the NSC, staffers were divided into seven different regions, with the following distribution of staffer personnel: Asia (6), Africa (4), Europe (6), Southeastern Europe (6), Russia/Ukraine (6), Inter-American (5), and Near East and South Asia (4).

Third, NSC staffers also have a role in formulating defense policy.[123] They are tasked with taking into consideration how to place US strategic forces as well as theatre, naval, and special forces—bearing in mind important questions of strategic mobility as well as command and control communications.

Fourth, NSC staffers consider political and military affairs, which includes assessing and analyzing low intensity warfare policy, counterterrorism policy, and security assistance and alliance security policy.

Fifth, NSC staffers consider questions of arms control policy. Often overlapping to some extent with defense policy, arms control policy questions typically revolve around ways to manage strategic forces, theatre and conventional forces, as well as outer space.

Sixth, NSC staffers deal with questions of economic, scientific, and technological affairs relating to the security issues the United States faces. It is important to note that so-called "non-traditional security threats" are also a large component of NSC calculation upon which military, informational, economic, and diplomatic variables are managed.[124] Such threats pertain to medical security, drugs, immigration, trade, international monetary conduct, development aid, energy and resource security, strategic communications, and telecommunications and data processing.

---

[122] Worley, *Orchestrating the Instruments of Power*, 358.
[123] Carnes Lord, *The Presidency and the Management of National Security*, 61-68, 115-146.
[124] Cynthia Watson, *US National Security: A Reference Handbook, Second Edition*, 8.

Seventh and lastly, NSC staffers handle intelligence matters—from the perspective of policymakers acting independently of the IC. Note that in this area in particular, overlap with the US Intelligence Community (IC) can be considerable at times. NSC staffers assigned to handle intelligence matters address issues of current intelligence, intelligence policy and resources, special intelligence-related covert operations, counterintelligence, and strategic security. One historical example demonstrating this potential for overlap was the creation of the Executive Committee of the National Security Council (EXCOMM). EXCOMM was a special NSC subcommittee consisting of a mix of NSC members and representatives of the IC to advise President Kennedy during the 1962 Cuban Missile Crisis.[125]

Informal Structures and National Security Decision Making Theory

As the previous section has demonstrated, intelligence flows into the formal structures of national security decision-making from all tiers of the NSC. The IC is tasked with producing finished intelligence products for policymakers at all levels, but the sheer quantity of information the IC processes on a daily basis necessitates a system of management to handle what reaches the NSC. Staffers take the responsibility of handling this "grunt work" and ensuring that their superiors gain access to intelligence pertinent to the decision-making they must make. The thesis will explore in greater depth in Chapter Five the means by which this intelligence flows, and the difference made by OSINT. For now though, the chapter proceeds to deconstruct the second major component of the national security decision-making variable: informal structures.

[125] David A. Welch, and James Blight, "The Eleventh Hour of the Cuban Missile Crisis: An Introduction to the ExComm Transcripts," *International Security* 12, no. 3 (1987-1988): 5-29.

Formal structures, as established by the 1947 National Security Act and subsequent legislation, have shaped the National Security Council into the complex bureaucratic entity that it is today. However, in addition to the formal-institutional structures that contribute to national security decision-making, so-called informal structures exist as well and play equally if not a more important role in the decision-making process.[126] Whereas formal structures largely relate to the operation of the National Security Council, informal structures predominantly considers the role of the President of the United States as a single actor in the decision-making process. In detailing what is meant by "informal" structures, this section will also begin transitioning to discussing the broader topic of means of modeling national-security decision-making that produces the most optimal policy outcomes.

It is important to first establish that national security decision-making is not a static process.[127] It often faces adjustments when the standard procedures of the formally structured system do not serve the security or political purposes of the requirement of decision-makers. Presidents in particular often find themselves in positions where adjusting decision-making structures proves desirable when standard interagency procedures no longer serve their political purpose. Two major schools of thought on presidential national security decision-making presently exist: (1.) *institutional approach* and (2.) the *idiosyncratic approach*.[128]

The institutional approach fundamentally argues that the international and

[126] Karen M. Holt, "Strengthening Presidential Decision-Making Capacity," *Presidential Studies Quarterly* 30, no. 1 (2000): 35.
[127] William W. Newmann, "The Structures of National Security Decision Making: Leadership, Institutions, and Politics in the Carter, Reagan, and G.H.W. Years," *Presidential Studies Quarterly* 34, no. 2 (2004): 272.
[128] Names for these two schools of thought partially adopted from, ibid., 275-276.

political context in which a president operates is essentially the same, and therefore decision-making in all presidential administrations reflects similar structural dynamics.[129] Institutionalism views decision-making processes largely as a competitive struggle for control of policy between government officials and cabinet departments within established bureaucratic structures.[130] It argues that policy choices are made through negotiations among these officials in departments. While it is not exclusively a theory of formal national-security decision-making structures, the theory acknowledges the importance of administrative structure in shaping and influencing the informal structures of bureaucratic competition.

The idiosyncratic approach, on the other hand, turns away from bureaucratic competition and instead focuses on the personal leadership style of the president himself.[131] It argues that this personal leadership style in each president is the key variable in national-security decision making. The theory stresses that all presidents are unique actors and will devise very personal ways of making decisions. In order to create a functional national security decision-making system, the theory suggests that decision-making processes must be established to fit the president's individual beliefs. Scholars have devised different models on the characteristics of presidential management style. For example, Johnson has argued a president manages by fostering a competitive, collegial or formalistic environment[132] while Porter has sustained that presidents manage their subordinates through centralized management, "adhocracy", or multiple-

[129] Ibid.
[130] In scholars Fred Block and Mathew R. Keller's book *State of Innovation: The US Government's Role in Technology*, theories of internal bureaucratic competition are considered in the context of what the authors coin as "industrial policy." For more on their theory of informal national security decision making see Fred Block and Mathew R. Keller, *State of Innovation: The US Government's Role in Technology*, New York: Routledge, 2011.
[131] Newmann, "The Structures of National Security Decision Making," 275-276.
[132] Richard T. Johnson, *Managing the White House*, New York: Harper and Row, 1974.

advocacy.[133]

Considering historical examples of the "idiosyncrasies" of presidential leadership will better help to conceptualize what exactly is meant by the idiosyncratic approach. Consider the following three, consecutively serving, presidents: Jimmy Carter, Ronald Reagan, and George H.W. Bush.[134] Each of these three presidents had their own unique ways of receiving information and advice, making decisions, and involving himself in the process of national security decision-making. Influences shaping the diversity of these preferred idiosyncratic means of operation are likely results of various psychological factors such as cognitive style, development during childhood, and lessons learned from historical experiences inside and outside of government.

Jimmy Carter sought to move the NSC back to its Eisenhower years "golden age" by attempting to reverse the trend of using NSC staff as a replacement for foreign aid and defense policy bureaucracies.[135] He sought to move national security decision-making of the NSC back to being the main purview of the presidential cabinet. Carter had a tendency to micromanage NSC affairs, seeking to be very active and involved in the decision-making process.

Ronald Reagan's approach and style was the polar opposite of Carter's.[136] Reagan approached national security decision-making with a "detached" and "hands-off" attitude, preferring to set overall policy themes ("the big picture") rather than micromanage on the level Carter perhaps intentionally and unintentionally did. Reagan left an

[133] Roger Porter, *Presidential decision-making: The economic policy board*, New York: Cambridge University Press, 1980.
[134] Examples taken from, Newmann, "The Structures of National Security Decision Making, 281-282.
[135] Jerel A. Rosati, "Jimmy Carter, a Man Before His Time? The Emergence and Collapse of the First Post-Cold War Presidency", *Presidential Studies Quarterly* 23, no. 3 (1993): 459-476.
[136] Dale L. Smith, "Reagan's National Security Legacy: Model Based Analyses of Recent Changes in American Policy", *The Journal of Conflict Resolution* 32, no. 4 (1988): 595-625.

unprecedentedly large degree of power to his senior advisers to independently make many tactical national security decisions as well as manage implementation details of broad policies.

George H.W. Bush's presidential leadership style was a mix between the styles of Carter and Reagan.[137] Bush perhaps was one of the most experienced presidents in foreign policy and national security decision-making of any president: serving time as US ambassador to the United Nations, Chief of the US Liaison Office to the People's Republic of China, Director of Central Intelligence, and Vice President of the United States. Bush implemented a national security decision-making system in which all decisions were to be made on an interagency basis, with no departments or points of view to be excluded. The atmosphere of his style was overall informal but simultaneously very involved.

With these two national security decision-making schools of thought in mind and considering historical instances of the idiosyncratic approach, theorists have developed conceptual models for how decisions are made and what causes change in national-security decision-making. Before exploring two major models, a review of the broader idiosyncratic approaches to national security decision-making that may or may not contribute to optimal policy results is first necessary.

Traditional theory of national security decision-making centers on the rational actor decision-making model. This model is most often associated with institutionalism and the formal structures of decision-making: that is, that national-security decision-making is a rational and linear process of stating objectives, ranking values, analyzing

[137] Curt Smith, *George H.W. Bush: Character at the Core*, Lincoln: University of Nebraska Press, Potomac Books, 2014, 158-190.

alternatives, examining consequences, and making choices—in that order. This theory also posits that the rational actor model of decision-making is the most ideal way to produce optimal policy results.[138] Scholars of this traditional, institutional way of analyzing national security decision-making include Lindblom[139], Snyder[140], Braybrooke and Lindblom[141], Schelling[142], Allison[143], Schelling[144], March[145], et al.

Since 1947 and even earlier, scholars who have found merit in the rational-actor institutional approach have also asserted that the principal arguments of the idiosyncratic approach apply in tandem with the principles of rational-actor institutionalism (e.g. Lindblom).[146] Simon[147] for example, argued that while objective "facts" in an ideal world form the basis of organizational-decision making, "values", even in an un-ideal world, also play a part. Simon adds that a decision is not a simple unitary event, but the product of a complex social process generally extending over a period of time. Lindblom[148] added to Simon's idea on the importance of values, positing that "values" in principle cannot be separated from concrete policies. He also argued that informational, resource-related, and time constraint realities that all national security decision-makers face often break down

[138] James P. Pfiffner, "Presidential Decision Making: Rationality, Advisory Systems, and Personality", *Presidential Studies Quarterly* 35, no. 2 (2005): 217-218.
[139] Charles E. Lindblom, "The Science of 'muddling' through,'" *Public Administration Review* 19, (Spring 1959): 79-88.
[140] Glen Synder, *Deterrence and Defense*, Princeton: Princeton University Press, 1961.
[141] David Braybrooke and Charles E. Lindblom, *A Strategy of Decision*, New York: Free Press, 1963.
[142] Thomas C. Schelling, *Arms and Influence*, New Haven: Yale University Press, 1966.
[143] Graham Allison, *Essence of Decision: Explaining the Cuban Missile Crisis*, New York: HarperCollins, 1971.
[144] Thomas C. Schelling, *The Strategy of Conflict*, New Haven: Yale University Press, 1980.
[145] James G. March, *A Primer on Decision Making*, New York: Free Press, 1994.
[146] Note however, that as the discussion to follow will make clear, a good number of these *rational-actor institutionalism plus* or idiosyncratic theories were developed rather recently and distant from from the so-called "golden age" of rational-actor institutionalism (e.g. 1960-1980). See Pfiffner, "Presidential Decision Making", 217-228.
[147] Herbert A. Simon, *Administrative Behavior: A Study of Decision-Making Process in Administrative Organizations*, New York: Free Press, 1945.
[148] See Lindblom *supra*.

the ideal functioning of rational actor institutionalism.

Rational-actor institutionalism[149] was also partially deconstructed by theory on "advisory systems", or the idea that since no one rational individual president can realistically ever hope to understand all of the possibilities and ramifications of decision-making, he must rely on staff structures to help advise the decision-making process. This deconstruction sustains that informal advisory systems structuring idiosyncratic decision-making produce the most optimal policy results.

However there is a caveat. Advisory systems also have potential to *hinder* good decision-making. While some scholars of advisory systems, like President Eisenhower[150], have argued that advisory systems always produce optimal outcomes by minimizing the chances of decision-making "stalling", many others cite subjective, value-related issues as an endemic problem making this outcome unlikely.

Scholars writing after Simon, Lindblom, and Eisenhower took further interest in the concepts of "values" and "advisory systems." George[151] and George[152] are credited with bridging the gap between theories on "values" and theories on "advisory systems" by developing a new concept of "multiple advocacy."[153] George's theory asserts that presidents need to assure that their advisory systems provide them with a range of alternatives for any important decisions and that the best way to assure this is through a system of multiple advocacy, or "a strategy of role tasks and process norms to guide…decision-makers towards an optimal decision-making process"—allowing the

[149] For an alternative theory on national security decision-making that departs from rational actor institutionalism see Alex Mintz, "How do Leaders Make Decisions? A Poliheuristic Perspective", *The Journal of Conflict Resolution* 48, no. 1 (2004): 3-13.
[150] Dwight D. Eisenhower, *Waging Peace*, Garden City: Doubleday, 1965.
[151] Alexander L. George, "The case for multiple advocacy in making foreign policy," *American Political Science Review* 66, no. 3 (1972): 751-85.
[152] Alexander L. George, *Presidential decision-making in foreign policy*, Boulder: Westview Press, 1980.
[153] See Johnson *supra*.

president to make an independently informed policy choice as a result of having heard a variety of opinions debated freely, informally, and openly among advisors.[154]

However, it was immediately during the shaping of "multiple advocacy" theory that its flaws, originally deriving from the biases of advisory systems theory, would be assessed. Assessment of these flaws indirectly led to the emergence of the idiosyncratic school of thought, as it exists today. Janis[155] posits that multiple advocacy often falls victim to "groupthink." "Groupthink" is a pattern of thought characterized by self-deception, forced manufacture of consent, and conformity to group values and ethics.[156] Janis argues that the effects of small-group solidarity that naturally characterize multiple advocacy and their advisory system institutional apparatuses are exceptionally impactful during national security decision-making situations when stakes are high, pressure is great, and secrecy is important. Janis identifies the danger of these situations in that the group making decisions has a tendency to develop an illusion of invulnerability, infallibility, and possession of inherent morality. In these situations, groupthink often results in underestimations of adversaries and the chances of failure due to a failure to reexamine initial assumptions.

The idiosyncratic approach to national security decision-making explains why the groupthink effects of multiple advocacy frequently lead to the policymakers of advisory systems excessively tailoring decision-making to reaffirm a president's preexisting beliefs and conceptions of national security.

---

[154] A. Alexander Moens, "The Multiple Advocacy Strategy and the Role of the Custodian: the Carter Years", Paper presented at the Faculty of Graduate Studies (Department of Political Science) The University of British Columbia, Vancouver, Canada, January 1988, ii.
[155] Irving Janis, *Groupthink: psychological studies of policy decisions and fiascoes*, Boston: Houghton Mifflin, 1982.
[156] "The definition of 'groupthink', *Merriam-Webster Dictionary* (Boston, MA), Accessed Feb. 10, 2019.

However, despite this reality, multiple advocacy has potential to avoid the pitfalls of groupthink and produce optimal policy outcomes. The theory asserting that the idiosyncratic approach to national security decision-making can be adopted in a manner circumventing[157] groupthink is called the theory of the neutral/honest broker.[158]

Neutral/honest broker theory argues that in an ideal situation any given member of a national security decision-making system of multiple advocacy will present to the president in a neutral way important policy alternatives. The theory adds that this type of adviser will represent *faithfully* the views of the advocates of different policy alternatives.[159] If top staffers do not carefully play a neutral broker role but instead become subjective policy advocates, not only does groupthink become a greater possibility but also the burden shifts to the president to assure that all legitimate perspectives are well represented. This brings forward a second risk to the effectiveness idiosyncratic approach. If other staffers are not confident that their views are being accurately presented to the president, they will tend to find their own backchannels and undermine the order of the policy process.

Putting it All Together: Modeling National-Security Decision-Making

Up until this point, the history of national security decision-making has been reviewed and a deconstruction of the national security decision-making variable, into its

[157] National security decision-making scholar Karen M. Holt makes the case that presidential decision capacity can be judged generally to have increased when decision-making is: (1.) more representative; (2.) more procedurally rational; and (3.) more accountable. The neutral/honest broker can be defined as an advisor that embodies an optimal degree of representativeness, procedural rationality, and accountability. For a detailed discussion of what the qualities of embodying these characteristics entail see Holt, "Strengthening Presidential Decision-Making Capacity,"29.

[158] For a work that comprehensively covers a historical analysis of neutral/honest broker theory again I recommend, Burker, *Honest Broker?: The National Security Advisor and Presidential Decision Making*. See *supra* n. 123.

[159] Pfiffner, "Presidential Decision Making: Rationality, Advisory Systems, and Personality", 219-220.

formal and informal structures, has been posited. The discussion now turns to the topic of ways to model national security decision-making so that decisions made produce optimal policy results. Two major, broad theoretical models of national security decision-making will be discussed.[160]

The first model is the Walcott and Holt model.[161] This scholarly duo makes the argument that three different sources of decision-making structure exist: (1.) political environment, (2.) presidential choice, and (3.) organizational dynamics. They sustain that these structures acting in tandem produce optimal policy results.

Walcott and Holt argue that political environment has both an international and domestic context. On presidential choice they make the case that a president's political objectives and strategy bear great influence on the context in which a president makes a national security decision. Regarding organizational dynamics, Walcott and Holt posit that relationships between officials, departments, and the president impact the way in which a national security system is both institutionally and idiosyncratically organized. Their model recognizes both the importance of values, which forms the basis of the idiosyncratic approach, and the structure that defines institutionalism. It also takes into consideration a factor not previously discussed: international political environment. While one might idealize national security decision-making as a totally insular means of responding to external developments, it is also important to explicate that the process of responding to external stimuli is not made in a vacuum of domestic isolation.

---

[160] While far more than two comprehensive models on national security decision-making certainly exist, I have selected two-models to discuss in this section: that of Walcott and Holt (1995) and that of Newmann (2004). I have selected these two models (of which, Newmann's model has greater merit) because they most logically follow from the previous discussion on institutionalism, the idiosyncratic approach, advisory systems, multiple advocacy, etc.

[161] Charles E. Walcott and Karen M. Holt, *Governing the White House,* Lawrence: University Press of Kansas, 1995.

William Newmann developed a model of his own as an alternative to the Walcott-Holt model.[162] Newmann's model distinguishes itself from the Walcott-Holt model first and foremostly in structure. While the latter model largely organizes itself in the context of values and structural background, the former model is divided into theories of style, strategy, and structure. The Newmann model further distinguishes itself by subdividing structure based on the interagency process that inherently defines the institutional structure of the NSC. Newmann divides the NSC-system into *formal structure*, *informal structure*, and *confidence structure*. He argues, like Walcott and Holt, that when acting together, these structures produce optimal policy results. Formal structure is synonymous with the standard interagency process of various government agencies, departments, and other actors making structured national security decisions based on a tiered system of the president, the NSC proper, Principals, Deputies, and staffer working groups. Where formal structure principally refers to the way decisions are made institutionally, informal structure refers more to the idiosyncratic approach. Informal structure, according to Newmann, is simply when senior advisors meet with a president, outside the tiered system of the NSC. Newmann's third structure, the confidence structure, is defined as a more restrictive form of the informal structure. The scholar argues that confidence structures exist when a president relies almost exclusively on one or two most trusted senior advisors to make senior policy decisions.

Newmann continues developing his model with a three-pronged approach similar to that of Walcott and Holt's.[163] He further sub-divides his model into: (1.) management style, (2.) leadership style, and (3.) political strategy. Management style is an explicit

[162] Newmann, "The Structures of National Security Decision Making, 272-275.
[163] Ibid.

recognition of the "overall design" or formal structure of a national security decision-making system (i.e. NSC, Secretary of State, Assistant to the President for National Security Affairs, etc.). Leadership structure is Newmann's way of recognizing the idiosyncratic elements of presidential decision-making. He defines leadership style as the ways in which presidents are involved in the decision-making process, and how the president relates to his advisers as a group, individually. Lastly, on political strategy Newman somewhat vaguely cites "political strategy" as an important consideration. Citing Alfred Chandler's theory that "structure follows strategy"[164], he makes the case that strategy in general ultimately shapes the way in which policymakers shape structures, which in turn determine whether or not national security policy objectives are achieved.[165]

As with Walcott and Holt's model, Newmann's model bears consideration in defining a new perspective.[166] The model does well where the Walcott and Holt model does not by separately defining structure types as they derive from the NSC decision-making process, although the inclusion of a "confidence structure" appears to be somewhat redundant. At best, one could place confidence structure as a subdivision of informal structure. Structurally distinguishing a president's relationship with one or two of his most trusted advisors, as opposed to the relationship he forms with his senior advisors, is inappropriate and risks over compartmentalizing the national-security decision making process. Stated simply, a president's confidence structure *falls within* his informal structure.

---

[164] Alfred Chandler, *Strategy and Structure*, Cambridge: MIT Press, 1962.
[165] Note that when Newmann refers to "strategy" his assumption is that he refers to both "grand strategy" as well as domestic strategic considerations in shaping the formal structures of national security decision-making apparatuses.
[166] See Chapter Seven: The Cuban Missile Crisis of 1962.

On Newmann's redefinition of the three sources of decision-making structures of Walcott and Holt, he paints an overly broad and somewhat repetitive picture of decision-making sources. For example, his points on "management style" and "political strategy" more or less state the same idea that sources of decision-making relate to overall structural design. These points could be consolidated and subdivided by the three forms of NSC-based decision-making structures he outlines. His point on leadership style likewise bears significant resemblance to Walcott and Holt's point on organizational dynamics. However, Newmann can be praised for broadening the role of the president in decision-making beyond political objectives and strategy to individual relationships between the president and each of his senior advisors.

Conclusion

With the forgoing discussion of national-security decision-making and the structural considerations that may lead to more optimal policy results, the conclusions reached by this chapter can now be summarized in full.

Beginning with the unprecedented global nature of the conflict that was the Second World War and culminating with the passing of the 1947 National Security Act, the dominant conception of security in the United States has drastically changed from security seen as a basic constitutional principle of protecting the territorial sovereignty of the state to a new perception of security as a concern with global implications.

National security decision-making can be approached from two different theoretical directions: through a formal, institutional means or an informal or primarily idiosyncratic means. To assert that only one of these approaches accurately defines the

greater national security decision-making process as a whole ignores the fundamental reality of the history of the national security state—that national security decision-making involves a dynamic mixing of formal structures and informal structures that shape, alter, and oftentimes distort policy decisions.

The statutory establishment of the National Security Council largely defines the formal structure of the US national security decision-making process. The tiered system of the NSC ensures, at least in theory, that questions of national security decision-making are answered from a variety of approaches: from the narrow technical expertise of NSC staff members organized in working groups to the broad, policy-oriented final decisions made by the Council proper and the President of the United States himself. It is in the formal structures of national security decision-making that intelligence of the IC flows most freely.

In the background of the formally structured decision-making environment one finds a great deal of informal decision making put into practice as well. While the rational-actor model explains in theory why the formal structuring of the NSC should be efficient, a rigid interpretation of the model neglects to take into account the important reality that decision-makers often act irrationally due to cognitive biases, values-motives, and the effects of advisory systems and multiple advocacy. Informal structures do not *guarantee* that national security decision-making falls victim to these effects, such as groupthink. Often times informal structures lead to policy advocates adopting an honest/neutral broker advocacy approach, which can circumvent the pitfalls often associated with informal national security decision-making structures.

Lastly, scholars have sought to model national security decision-making in a

variety of ways. This chapter considered two such models: that of Walcott and Holt and that of Newmann. While both models merit commentary and get pieces of the overall decision-making picture correct, neither equitably balances the factors that play into how national security decisions are ultimately made.

To summarize, national security decision-making is based on a blend of two structural considerations: that of formal structure and that of informal structure. Formal structure can be defined as the statutory-established mechanisms that define national security decision-making. Formal structure primarily consists of the functioning of the National Security Council, but also includes the functioning of other national security-related interagency interactions within the federal bureaucracy as well as within the structure of the US Intelligence Community. Informal structure, on the other hand, can be defined as the personal leadership styles and personal relationships presidents (and other high ranking policy decision-makers) form that indirectly or directly contribute to the decision-making process. Informal structure takes into consideration cognitive biases, preferred leadership environments, and other inter- and intrapersonal values that shape decision-making.

Furthermore, one may subdivide decision-making structures into three additional influences on decision-making: organizational dynamics, political environment, and structured-institutional management style. The first two influences branch from informal structures. Their definitions are adopted from Walcott and Holt. However, I add a new category, from the "management style" prong of the Newmann model: structured-institutional management style. Beginning with the definition of management style that Newmann provides—that is, the "overall design" of an administration's decision-making

process—I qualify that overall design in this case comes from statute-established decision-making formal structures like the NSC and the US Intelligence Community.

With these general and more specific conclusions drawn, the thesis turns next to considering the nexus between the two variables of Chapters Three and Four. Chapter Five will transition from examining the individual variables of OSINT and national security decision-making to examining the relationship between the two in tandem. The end result of Chapter Five will be a final statement answering the principle research question this part of the thesis seeks to address.

CHAPTER FIVE: THE NEXUS

To review, the purpose of the previous two chapters was to define, deconstruct, and independently analyze the two variables the thesis seeks to consider: the OSINT discipline and national security decision-making. With these variables sufficiently established, now the two can be considered in tandem. As a reminder, Part One of the thesis, but this chapter in particular, seeks to answer the following question:

> What is the relationship, if any, between the Open Source Intelligence (OSINT) discipline and national security decision-making in the United States of America?

This chapter will recapitulate the major points of what has been established so far and in doing so will attempt to deduce the relationship between OSINT and national security decision-making. The chapter will conclude by explicitly answering the research question and beginning to discuss how the conclusions drawn in this chapter will be utilized in Part Two of the thesis to come.

Recapitulation and Deductions

Beginning with the recapitulation, a new definition of OSINT was defined in Chapter Three. This definition defined OSINT as:

> [T]he intelligence discipline in which publicly available or legally accessible information is synthesized through the intelligence cycle of collection, exploitation, analysis, classification, and dissemination in order to meet a specific intelligence consumer requirement.

As established, OSINT is not a static process, and while it may be considered as a monolithic *variable*, it is far from being a monolithic *entity*. A number of stages and actions take place in the process of transforming OSINF into OSINT. OSINF is collected by a variety of technologies and means; exploited for relevant material suitable for analysis; analyzed by experts and compiled in reports, tables, and graphics; is classified; and its final products are eventually distributed to policymakers.

As a reminder, there are two major coexisting structures that simultaneously define national security decision-making in the United States: formal and informal structures. Formal structures are statutory established mechanisms that constitute a bureaucratic structure in which national security decision-making is made. Informal structures are the personal leadership styles; the bureaucratic relationships and competition among agencies of the formal structure; and personal relationships high-ranking policy decision-makers form that directly and indirectly contribute to decision-making.

The formal structures of decision-making mostly consist of the National Security Council (NSC), although among Council members are heads of departments of the government and agency leaders within the United States Intelligence Community (IC). Examples of this include the NSC membership of the Secretary of Defense (e.g. Defense Intelligence Agency), the Secretary of State (e.g. Bureau of Intelligence and Research), and the Secretary of the Army (e.g. Army Military Intelligence), the Secretary of the Navy (e.g. Office of Naval Intelligence), and the Secretary of the Air Force (Air Force Intelligence, Surveillance, and Reconnaissance). As OSINT is not an agency-exclusive discipline, one can deduce that to at least some degree that finished intelligence products

of OSINT enter the formal national security decision-making structure in some capacity, either from FBIS's successor agencies or from other agencies.

The NSC serves as a means of providing information to decision-makers for crisis management, information for policy development and implementation, and information for policy advice. While policymakers can be informed by department reports, polling, and verbal presentations by their advisors, intelligence serves as at least an equally important means of receiving the necessary information for these decisions. Issues of national security are often of a sensitive nature so as to necessitate "secret" intelligence, which typically the IC is only capable of providing. This does not mean however that the IC does not utilize raw intelligence of the open source variety in its reports, especially in its all-source intelligence reports. Open source information by definition is available to all members of the public. However, corroborating publically available information with information that remains private often facilitates making sense of open source information and giving it intelligence value.

In many regards, the theoretical sequence of events in which OSINF becomes OSINT bears similarities to the theoretical sequence of events in which the formal structures of national security decision-making operate. This is most evident in the tiered structure that fundamentally defines the NSC. Intelligence produced by the IC that makes its way into the NSC system flows to all three of the major tiers of the structure: the President and his closest advisers level, the NSC Principals and Deputies committees, and the NSC staff. Often intelligence that flows into the system begins at the staffer level. Many of the central functions of NSC staff involve utilizing information to make decisions. For example, NSC staffers are tasked with reviewing strategic intelligence for

policy assessments; making recommendations for long range strategic planning; making recommendations for short-range crisis advice; formulating defense policy; making recommendations on political and military affairs; advising on arms control policy; and providing recommendations on economic, scientific, and technological affairs (e.g. medical security, drugs, and immigration). All of these tasks, especially the first listed, directly involve NSC staffers interacting with intelligence—which can come from the products of the OSINT intelligence discipline. Staffers are specifically tasked with exclusively handling intelligence matters as well. Staffers regularly consider policy options available from current intelligence, intelligence policy and resources, special intelligence related to covert operations, counter terrorism intelligence, and strategic security intelligence. OSINT, like all intelligence disciplines, concerns itself with providing finished intelligence products on all of these functional types of intelligence.

But do finished OSINT products flow as abundantly into the informal structures of national security decision-making as they do in formal structures? As detailed, informal national security decision-making structures can be subdivided into the institutional and the idiosyncratic. Institutionally speaking, there is reason to believe that the internal competition between the various departments and agencies of the federal government hinder the effective channeling of OSINT products into national security decision-making. Agency and department competition and tampering with IC procedure to ensure that finished intelligence products of other disciplines reach policymaker desks may in fact result in a deliberate displacement of more relevant finished intelligence of the OSINT variety –to the detriment of the policymaker who makes better-informed decisions with a greater variety of sources and higher quality, finished intelligence

products.

From the idiosyncratic perspective, it has been established that some policymakers will be more receptive to OSINT products than others due to a mix of environmental factors, personal preferences, and cognitive biases. Returning to the leadership decision-making styles of Presidents Carter, Reagan, and H.W. Bush, one can see how the degree of a president's personal interaction with representatives of the IC providing intelligence can vary depending on presidential leadership styles and preferences. While formal structures theoretically ensure steady flow of intelligence to policymakers, informal structures do not always guarantee this—a policymaker's receptivity to intelligence varies from policymaker to policymaker.

The idiosyncratic perspective's view on advisory systems bears consideration as well. In theory, while the web of intelligence sharing is certainly not perfectly hierarchical in practice, ideally all higher tiered national security decision-makers of the NSC panoply receive at least some of their intelligence from those below them. This indicates that to some degree finished intelligence products, including OSINT products, are filtered as they move from IC analysts and NSC staffers to the desks of department heads and the president himself. What gets into the hands of policymakers depends in part on what their advisors draw their attention toward. As established, multiple advocacy can be detrimental to effective national security decision-making (e.g. groupthink attitudes) or beneficial (e.g. honest/neutral broker). The OSINT implication of this theory is that OSINT products that enter the national security system (formal or informal) have potential to be underutilized, "lost", or distorted as they move among the tiers of decision-making and are influenced by advisory systems.

One cannot ignore the impacts of the other influences that impact decision-making: organizational dynamics, political environment, and structured-institutional management style. OSINT, by the "open" or "un-secret" nature of the information it deals with, has often been unfairly devalued in comparison to the secret and classified information other disciplines process. National security decision-making structures and management that deliberately underutilizes or shelves OSINT because of these biases hinders the impact of OSINT finished products on policymaker decision-making. One example of this phenomenon is the continued nonexistence of an exclusively OSINT branch of the IC. From FBIS's heyday to today's Open Source Enterprise, OSINT remained and remains under the purview of the Central Intelligence Agency –meaning OSINT producers have traditionally had to pass through CIA bureaucracy to get their intelligence directly to policymakers.

OSINT's very nature gives it a flexible range of nontraditional uses that have greater potential to better inform policymakers tasked with making national security decisions. This new potential is conditioned on the continued, and expected, development of new technologies to improve the collection phase of OSINT. Commercial off the shelf (COTS) tools–while originally used by private sector firms for advertising, brand management, and consumer analytics purposes –are increasingly being incorporated into the OSINT discipline. The typical linguistic and content-based programs of COTS tools could have greater use in the OSINT discipline than in other disciplines more concerned with acquiring "secret" information. These COTS tools, as well as less technologically complex uses of social media and the Internet, also have potential to improve counterintelligence capabilities of the IC and the national security community of

policymakers in which it serves. OSINF can be used defensively as well as offensively to conduct counterintelligence operations. As the experiment of Haynes and Cappa attests, OSINF can be collected to meet OSINT counterintelligence needs. A future, independent OSINT-focused agency of the IC could develop its own counterintelligence division similar to the CIA's Special Activities Division, largely responsible for covert operations.

It is important to note in defining OSINF that open source material has several ways of being obtained: through formal request, purchase, or observation. All three of these activities are not only conducted by intelligence agencies of the IC, but virtually by every agency of the federal government. In 2019 virtually every federal government agency has one or more social media pages where it can monitor the activity of users that interact with it. Government agency press offices constantly keep up with the flood of news media content so they can respond to and field questions of current events issues relating to their activities. Governments not only produce but also procure gray literature. OSINT also serves as a means of fostering greater interagency unity within the IC, which in turn would help to reduce the bureaucratic stovepipes problem that national security decision-making in the US faces. The open nature of OSINF means that virtually every agency of the IC could utilize it in an effort to produce more all-source intelligence products, or intelligence products, organizations, and activities that incorporate all sources of information and intelligence in the production of a final product.

Lastly, future technological developments in the so-called "semantic web" (i.e. direct and indirect machine processing of data, machine learning, and automated reasoning) could lead to a new, third generation of OSINT or a Web 3.0. A third generation of OSINT may serve to finally eliminate the stereotype that OSINT only

involves the simple monitoring of social media and foreign news media—possibly increasing the perceived value of OSINT for national security decision-makers. OSINT could very well become one of the most technically advanced intelligence disciplines of the IC and could provide national security decision-makers with intelligence of unprecedented national security decision-making value.

To conclude, OSINT plays a prominent but still marginal role in the formal structures that define national security decision-making. OSINT infiltrates all levels of formal national-security decision-making, mostly through NSC staffers that are tasked with handling the substantive details of national security matters that finished OSINT products often provide. OSINT's influence on the idiosyncratic ways in which national security decisions are made is less certain, but likely comparatively less substantial. Interagency competition, policymaker biases (including environmental factors, personal preferences, and cognitive biases), and agency biases against OSINT have potential to minimalize its role in informing national security decision-making. Advisory systems have potential to utilize OSINT for better or for worse: as a means of justifying groupthink or as a means of informing the honest broker.

A history of the intelligence discipline during the Cold War era and beyond reveals that OSINT has played a critical role in informing at least some high-level national security decision-making. The fundamentally flexible nature of the OSINT discipline also provides a potential medium for greater incorporation of COTS tools into intelligence and consequentially national security decision-making; counterintelligence capabilities of the IC and the greater national security community; and greater interagency cooperation across the IC. The rise of a new "third" generation of OSINT

seems likely. This new generation could bring an unprecedented degree of technological benefit to the collection and processing capabilities of OSINT, thereby dramatically increasing the value of the discipline to policymakers involved with national security decision-making.

Conclusion

Part One concludes with a final theoretical statement on the relationship between the OSINT variable and national security decision-making.

To recall, the national security decision-making perspective developed in the previous chapter considers national security decision-making based on two structural considerations: that of formal structure and that of informal structure. Formal structure can be defined as the statutory-established mechanisms that define national security decision-making like the functioning of the National Security Council. Informal structures were defined as the personal leadership styles and personal relationships presidents (and other high ranking policy decision-makers) form that indirectly or directly contribute to the decision-making process. Decision-making structures can be subdivided into three additional influences on decision-making: organizational dynamics, political environment, and structured-institutional management style.

To answer the principal research question of Part One, yes, there exists a relationship between the OSINT discipline and national security decision-making in the United States. Finished OSINT products flow into both the formal and informal structures of national security decision-making, but by nature of the organizational dynamics of formal structures and the often less structured-institutional management

style and political environment natures of informal structures, OSINT likely bears greater influence on national security decision-making with formal structures.

It is important to qualify that while the above theoretical conclusions of the *general relationship* between OSINT and national security decision-making can be deduced, going further, such as developing a specific theoretical *model* for the relationship between the two variables or how specifically finished and unfinished OSINT products of the discipline lead to optimal policy results, is not possible given the inherent difficulties of establishing a theoretical causal relationship between finished intelligence derived from any one collection discipline and the content of US foreign policy.[167] The following chapter will try to address this inherent difficulty by attempting to apply a quantitative methodology to a historical case study.

This concludes Part One. Now the accuracy of this theoretical construction of the relationship between OSINT and national security decision-making will be put to the test quantitatively in Part Two, which will consider a historical case study on the Cuban Missile Crisis of 1962.

[167] For one work that clearly states the inherent difficulties of establishing a causal connection between intelligence estimates and foreign policy see Richard H. Immerman, "Intelligence and Strategy: Historicizing Psychology, Policy, and Politics," *Diplomatic History* 32, no. 1 (2008), 1-23.

PART TWO: A CASE STUDY: THE CUBAN MISSILE CRISIS OF 1962

"I am the wisest man alive, for I know one thing, and that is that I know nothing."

-Plato, *The Republic*

CHAPTER SIX: PART TWO METHODOLOGY

This second micro-chapter seeks to outline the methodology this thesis will employ in Part Two to answer its principal *quantitative* research questions relating to the relationship between the OSINT variable and the national security decision-making variable. The research questions for the thesis will first be explicitly listed. Following this, the methodology for conducting a quantitative experiment to test these questions will then be explained. The chapter will conclude with an explanation of how the conclusions drawn in Part One presented at the end of Chapter Five will be applied in the final chapter of the thesis to draw a general conclusion on all three research questions.

Research Questions

The research questions Part Two of the thesis seeks to answer can be divided into the following two questions on the relationship between the OSINT variable and the national security decision-making variable:

1. If the quantity and quality of open source information and finished open source intelligence products collected and produced respectively from the OSINT intelligence discipline *increases*, how does this impact national security decision-making?
2. If a causal relationship can be established between OSINT and national security decision-making, to what extent can it be established? When the *quantity* of OSINF/OSINT increases does national security decision-making produce more optimal policy results? When *quality* increases does national-

security decision-making produce more optimal policy results? When quantity and quality *both* increase, does national-security decision making produce more optimal policy results?

Testing Hypotheses

Unlike the first part of the thesis, the second part reports the results of a quantitative test of the fundamental relationship in question. The intention of this test was to evaluate the relationship between the OSINT variable and the national security decision-making variable that Part One of the thesis was unable to specifically deduce. The experiment proceeded as follows:

Phase One: Assessing Quality

I begin by assessing the value of 20 sampled Foreign Broadcast Information Service (FBIS) raw open source intelligence products and 10 different sampled finished intelligence products. I then assess each piece of raw and finished intelligence for quality based on the following four pre-defined criteria: *presentability, accuracy, actionability,* and *objectivity*. I then rank each piece of raw or finished intelligence, by criterion, a *quality points score* (QPS) between 1-5, with the lower number being the least of that characteristic and the higher number being the most of that characteristic. After all samples are ranked, I calculate the average QPSs for each category. I calculate separate averages for the 20 samples of raw intelligence and the 10 samples of finished intelligence (which I call "Quality Points Totals" or TQPs).

Phase Two: Assessing Quantity

I then develop a list of 10 different decisions the Kennedy Administration made

or could have made during the 13 days of the 1962 Cuban Missile Crisis, with each listed decision corresponding to a *possible* outcome from the decision. I then randomly select 5 of the 20 samples of raw open source intelligence, linking each piece of raw intelligence to decisions the decisions such information could have been used by EXCOMM to support. I note no connections if the information does not support any of the ten listed decisions. I then "select" the decision or decisions with the greatest number of connections as "the decision made" (DX), ultimately comparing the decision made to the decisions historically made on that matter by the Kennedy Administration in 1962 (DR). I then repeat the process, adding another 10 pieces of raw open source intelligence. I select a second DX, again to be compared to the DR. The process is repeated a third time, adding in the remainder of the raw intelligence. I select a third DX selected based on the quantity of connections, compared a third time to the DR. Note that I cumulatively sum the number of connections when more raw intelligence is added in each round.

Once I conclude this procedure with the raw OSINT, I then proceed to repeat the process again, starting over with the finished OSINT products. The same 10 decision-outcomes remain but now the connections added from the open source information phase of the experiment are set aside. The only procedural difference in this second round of testing is that I calculate DXs and DRs at the intervals of 3, 5, and 10 pieces of intelligence, in that order.

I then draw conclusions regarding quantity based on whether or not a larger inclusion of open source information and finished OSINT products led to decision making paralleling what the Kennedy Administration historically decided upon. *The key operating assumptions in this phase of the testing is that what actually happened (the*

DR) was the "best" possible outcome (i.e. no military exchanges or nuclear exchange and missiles removed—a victory for the Kennedy Administration against Khrushchev) and that the policymakers of EXCOMM engaging with the intelligence in question are interacting with it in a procedurally rational manner. There are certainly problems operating under this assumptions,[168] but for the practicality of having a benchmark to compare the DXs to, these are the assumptions I chose operate under.

Phase Three: Assessing Both Quality and Quantity

In the final phase of the quantitative test, I determine what happens if both quality and quantity increase *together*. I also consider whether the link between quality and quantity and better decision-making is causational or merely correlational. I achieve this by analyzing Phase One and Phase Two of the test simultaneously. I calculate the total number of quality points in each of the three rounds of Phase Two for both raw intelligence and finished intelligence based on the individual sample total quality scores (i.e. scores for each individual sample from all four quality criterion categories summed) with connections leading only to the Phase Two determined DXs. I sum these individual QPSs for grand QPSs for each of the six different rounds of Phase Two of the test. I then draw conclusions based on the six different grand QPSs as well as Phase Two comparisons to the DR to determine the effect both variables increasing (or decreasing) together have.

The final, concluding chapter of the thesis will qualitatively analyze the *quantitative conclusions* derived from the next chapter to the *theoretical conclusions*

[168] For example, on policymakers making decisions in a procedurally rational manner there is the issue of political decision making often not meeting the ideal standards of procedural rationality, as supported by the previous discussion on idiosyncratic approaches to decision making but also by, Brian Rathbun, "The Rarity of Realpolitik: What Bismarck's Rationality Reveals About International Politics," *International Security* 43, no. 1 (2018), 7-55.

derived from the previous chapter to make a final, cumulative statement on the three research questions posed.

CHAPTER SEVEN: THE CUBAN MISSILE CRISIS OF 1962

Before the quantitative test of the relationship between the OSINT variable and the national security decision-making variable of the 1962 Cuban Missile Crisis is presented, this chapter will begin with a historical section to contextualize the context of the case study selected. As implied by the discussion of methodology in the previous chapter, the test the thesis will present relies significantly on the historical context in which OSINT finished products were received by policymakers and national-security decisions were feasible. The first part of this chapter seeks to address, as much as reasonably possible, this essential historical context. The context regarding the general presence of intelligence and national security decision-making during the crisis, along with the work of FBIS at this time in its institutional history will be reviewed before the experiment itself is reported.

Overview: Intelligence, National Security, and the Cuban Missile Crisis

The Cuban Missile Crisis may indeed be one of the most studied events of the nuclear age.[169] Nonetheless, scholars have had a tendency to pay very close attention to the high politics of the missile crisis[170] but relatively little attention to its seemingly mundane operational dimensions, despite a large and growing quantity of primary source documents and records on these "minor" matters becoming declassified.[171] One might

[169] Amy Zegart, The Cuban Missile Crisis as Intelligence Failure, Hoover Institution Policy Review, Stanford, 2012.
[170] Pre-crisis, finished intelligence reports tended also to focus on the high politics of Soviet involvement in Cuba. As an example see Special National Intelligence Estimate: The Threat to US Security Interests in the Caribbean Area, SNIE 80-62, Washington, Jan. 17, 1962.
[171] James G. Blight, ed., and David A. Welch, ed, *Intelligence and the Cuban Missile Crisis*. New York: Routledge, 1998, 2.

include the operational role of the OSINT intelligence discipline in the crisis as such a "mundane" dimension. One may even classify the entire intelligence dimension of the crisis as a "mundane" component[172] largely overlooked by historians, scholars of political science, and scholars of international relations alike. This is alarming given that a fine pointed consideration of the historical record of the crisis proves the closest moment humanity ever reached to global nuclear war is largely a story of intelligence. From the dramatic U-2 flights of Major Rudolph Anderson and Captain Charles Maultsby to the mechanical chaos that almost led to the Soviet submarine B-59 launching its payload of T-59 nuclear tipped torpedoes at an American carrier group, the traditional narrative of the Cuban Missile Crisis often glosses over these "minor" tactical details pertaining to intelligence operations that almost resulted in a nuclear exchange.[173]

Although understudied, existing scholarship on the intelligence dimensions of the Cuban Missile Crisis tends to define the crisis as both an intelligence success and an intelligence failure. "Intelligence failure" can be defined as "a systematic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses".[174] The crisis is often seen as a failure because the United States Intelligence Community (IC) did not discover evidence of Soviet medium-range SS-4 and intermediate-range R-14

[172] Declassified finished intelligence documents have confirmed that the OSINT discipline was indeed utilized in producing intelligence for policymakers preceding and during the crisis. For one such report see Report to the President's Foreign Intelligence Advisory Board on Intelligence Community Activities Relating to the Cuban Arms Build-Up, Report of the Office of the Director of Central Intelligence, Washington, April 14-October 14, 1962. On collection resources utilized the report states that, "collection resources utilized included the overt press, radio and television."

[173] Although interesting, a full discussion of all the fine intelligence details that significantly played a part in defining the Cuban Missile Crisis would stray from the purpose of this chapter. Any readers interested in a very detailed hour-by-hour, day-by-day history of the crisis, particularly from an intelligence dimension, should consult either or both, Aleksander Fursenko, *One Hell of a Gamble: Khrushchev, Castro, and Kennedy, 1958-1964: The Secret History of the Cuban Missile Crisis*, New York: W.W. Norton & Company, 1998 and/or Michael Dobbs, *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War*, Visalia: Vintage Press, 2009.

[174] Rob Johnson, *Analytic Culture in the US Intelligence Community: An Ethnographic Study*, Collingdale: DIANE Publishing Company, 2005.

ballistic missiles until *after* they were deployed to facilities across Cuba.[175] The IC also did not discover until long after the crisis concluded that the Soviets had also deployed approximately 100 tactical (or "battlefield") nuclear tipped missiles for Soviet artillery rockets and Il-28 medium-range bombers on the island as well. However, scholars have also argued that the crisis can been seen as an intelligence success because thanks to U-2 imagery intelligence (IMINT) medium and intermediate range missile sites were discovered before they were rendered fully operational. U-2 flights after the initial October 15 discovery of the missiles sites additionally kept the IC and policymakers informed about the progression of the construction of the sites.

On the national security decision-making decisions of the crisis, much scholarly attention has been paid to the individual actors participating in EXCOMM.[176] A specific analysis of each individual actor's advisory reasoning during the crisis goes beyond the scope of this thesis, but it is important to note that thanks to what has already been declassified on the proceedings of the crisis management, a number of resources are available for scholars to better grasp who was thinking what and when.[177]

Before continuing the discussion in this chapter, a brief overview of the day-by-day progression of the crisis is useful. This sketch of what happened and when will be

[175] Blight, *Intelligence and the Cuban Missile Crisis*, 5. See also, Zegart, The Cuban Missile Crisis as Intelligence Failure, 33. Blight writes, "Before October 14, a PFIAB [President's Foreign Intelligence Advisory Report] report on the crisis finds that analysts did not publish any information indicating a potential offensive buildup in Cuba in the president's daily intelligence checklist [sic]."

[176] These participants were: President Kennedy, Vice President Lyndon Johnson, Secretary of State Dean Rusk, Secretary of Defense Robert McNamara, Secretary of the Treasury Douglas Dillon, Attorney General Robert Kennedy, Director of Central Intelligence John McCone, Chairman of the Joint Chiefs of Staff General Maxwell Taylor, Ambassador-at-Large Llewellyn Thompson, Special Counsel Theodore Sorensen, and Special Assistant to the President for National Security Affairs McGeorge Bundy. See Coleman, David. "NSC ExComm Meetings, 1962-1963". History in Pieces. https://historyinpieces.com/research/meetings-excomm-executive-committee-national-security-council (accessed March 1, 2019).

[177] The best available being, McGeorge Bundy and James G. Blight, "Transcripts of the Meetings of ExComm", *International Security* 12, no. 3 (Winter, 1987-1988).

useful for the reader's reference as the quantitative evidence of this paper is presented.[178] The follow table chronicles the crisis.

Table A: A Timeline of the Cuban Missile Crisis of 1962

Monday, October 15	Reconnaissance from U-2 aircraft reveals the locations of several SS-4 medium-range missile sites throughout Cuba
Tuesday, October 16	President Kennedy convenes an Executive Committee of the National Security Council or EXCOMM
Wednesday, October 17	U-2 reconnaissance produces photographs of an R-14 intermediate-range missile site
Thursday, October 18	The president meets with Soviet Foreign Minister Andrei Gromyko and states that the United States would not tolerate the presence of any Soviet nuclear weapons in Cuba; Gromyko denies the presence of any weaponry in Cuba
Friday, October 19	Kennedy meets privately with Secretary of Defense Robert McNamara and members of the Joint Chiefs of Staff to discuss possible military responses
Monday, October 22	Kennedy addresses the American public directly on the missile crisis in Cuba and announces his plans to implement a naval blockade to prevent further shipments of missiles to Cuba from arriving[179]
Tuesday, October 23	More U-2 reconnaissance photographs reveal that Soviet missiles are now ready for launch
Wednesday, October 24	Soviet ships en route to Cuba with missile site cargo are just about to approach the US quarantine line when these ships receive orders from Moscow to hold their positions in international waters just outside the blockade
Thursday, October 25	At the United Nations, US Ambassador Adlai Stevenson confronts Soviet Ambassador Valerian Zorin about the existence of the missiles
Friday, October 26	EXCOMM receives a letter from First Secretary of the

[178] Day-by-day account from, "Timeline of the Cuban Missile Crisis," Atomic Archive. http://www.atomicarchive.com/History/cuba/timeline.shtml (accessed: February 10, 2019.

[179] For an intriguing account of how the Kennedy Administration prevented the American press from publishing any significant reports on the crisis before Kennedy's October 22 address to the nation, see Shalom Sokolaw, "Publish and Perish? The Cuban Missile Crisis and Journalists' Right to Inform Versus Their Responsibility to Withhold", *New York History* 85, no. 3 (2004): 265-275.

	Communist Party of the Soviet Union, Nikita Khrushchev stating that the Soviets would remove their missiles if President Kennedy publically promises that under no circumstances the United States would invade Cuba
Saturday, October 27	The U-2 of Major Rudolf Anderson is shot down over Cuba; EXCOMM receives a second letter from Khrushchev stating that, in addition to a public promise not to invade Cuba, if the US also removes its Jupiter missiles based in Turkey, Khrushchev would order the missile sites in Cuba to be disassembled and their parts and components returned to the Soviet Union
Sunday, October 28	US accepts Khrushchev's offer, effectively ending the crisis; the final deal states that the missiles will be dismantled in exchange for the US promise to never invade Cuba and to take its own missiles out of Turkey

While the assessment of the IC's preparedness and response to the Cuban Missile Crisis was mixed both shortly following the crisis's conclusion and to this day, the contemporary reaction (and to a large extent the reaction today) views the event that brought the world to the precipice of nuclear was as a near total victory for President Kennedy.[180] Immediately following the crisis, opinion on the president's management of the crisis was overwhelmingly positive.[181] Congratulations poured into the White House form all over the world. Kennedy's popularity at home skyrocketed. His approval rating jumped from 61% to 74% and Democrats performed well in the November 1962 congressional elections, gaining a total of four seats in the Senate and losing only four in the House of Representatives.

This thesis seeks to consider the extent to which intelligence contributed to the national security decision-making "success" of the Cuban Missile Crisis. Note that the analysis to come does not seek to pass judgment on who "won" the crisis. This thesis

[180] Dominic Johnson, *Failing to Win: Perceptions of Victory and Defeat in International Politics*, Cambridge: Harvard University Press, 2006, 96.
[181] Ibid.

intends to consider a causal relationship, or lack thereof, between the OSINT variable and the national security decision-making variable.

The Foreign Broadcast Information Service: 1957-1967[182]

As established in Chapter Three, until 2005 FBIS was the principle intelligence agency[183] of the United States Intelligence Community devoted to utilizing the OSINT discipline to produce finished intelligence products for policymaker consideration. To the reader unfamiliar with the Foreign Broadcast Information Service (FBIS) it is important to contextualize, before the experiment itself begins, the operational history of FBIS. All of the "raw" intelligence that is considered was collected by FBIS. Considering this history gives greater insight into the background circumstances in which EXCOMM was receiving OSINT and all-source intelligence with OSINT components from the IC.

Between 1957 and 1967 FBIS expanded in its operations, with a number of new monitoring posts, new requirements, and new expenditures. The expansion was a result of a need to better incorporate new sources of information, to collect and analyze more

[182] This section's brief history of the Foreign Broadcast Information Service (FBIS) between the years 1957 and 1967 comes entirely from information obtained from the official internal institutional history of the organization itself: Foreign Broadcast Information Service History Part III: 1957-1967, Washington: The Directorate of Intelligence Historical Series, 1972. The 272-page publication, with minimal redactions, is the only significant source of information on the organization's internal operation in the years immediately preceding, during, and following the Cuban Missile Crisis. While I must entirely rely on this source for information on the history of FBIS during the time period of interest, I caution and advise the reader to bear in mind that the history of FBIS presented here is a history written by the subject of the historical analysis itself. As in any situation in which a historian writes an autobiographical history, note the obvious potential for bias, distortion, and exaggeration. This reality does not necessitate dismissing what FBIS has documented on its own operations. On the contrary, delving into the nearly 300-page history of the organization is worth any intelligence scholar's attention. Future corroboration of the myriad of statistics and operational details, if ever possible, even in part, is a task for future scholars of FBIS and OSINT.

[183] Note that although FBIS and its successor agencies should be designated an independent intelligence agency of the "seventeen agencies" said to make up the US Intelligence Community, its historical and present affiliations with the CIA have resulted in it not being included on this list. See Nina Agrawal, "There's more than the CIA and FBI: the 17 agencies that make up the U.S. Intelligence Community", *Los Angeles Times* (Los Angeles, CA), January 17, 2017.

information, and to improve quality of services. For example, between 1953 and 1960 the number of foreign radio transmitters used by FBIS expanded from 4,500 to 7,500.[184] Likewise, between 1955 and 1962 the hours of broadcasts collected from transmitters monitoring "communist" sources more than doubled.[185]

FBIS documented a large number of statistics on its operations and the operations of the adversaries of the United States during this period. A total of 12 FBIS stations were filling a little more than 200,000 words of broadcast material a day, 90,000 alone from the USSR and the Soviet satellite states of Eastern Europe.[186] USSR broadcast coverage jumped markedly during this period, from 485 hours weekly in 1956 to 566 hours in 1964. Those in China jumped from 189 to 451 hours during the same period.[187] FBIS determined that together with the British Broadcasting Corporation, it was listening to a total of six million words daily in 67 languages from 117 countries, compared to the only about two million words a day it listened to in 1947.[188]

FBIS's internal history shows that it was exceptionally interested in the activities of both Havana and Moscow between 1957 and 1967. Part of the reason for this was that both governments were producing a significant quantity of raw open source material at this time. By June 1963, the Castro regime was broadcasting propaganda continuously for about 19 hours a day in Spanish, Portuguese, and English.[189] By the end of 1964, Moscow had increased its broadcasts by 221 hours a week.[190]

FBIS notes that the 1957 to 1967 period was a time of reevaluating consumer

[184] Foreign Broadcast Information Service History Part III, 2.
[185] Ibid., 3.
[186] Ibid.
[187] Ibid., 4.
[188] Ibid.
[189] Ibid., 3.
[190] Ibid., 5.

wants. During this period, FBIS utilized its periodic "consumer survey" to determine what finished intelligence products its policymaker consumer desired as well as to weed out which subscribers had no real need for FBIS services. Consumer surveys during this time revealed that although consumers valued receiving the "full texts" of key speeches often included in finished intelligence products, they agreed that many speeches were largely "useless" and that the number of policymakers receiving FBIS publications needed to be reduced. To what extent FBIS responded to these recommendations is in doubt. For example, by the end of 1958 the "USSR and East Europe Daily Report" was issued to 664 users –an *increase* from the 1957 level of 624 users.[191]

The record also suggests that demand for FBIS intelligence increased between 1957 and 1967, especially regarding "special requests". Special requests were made for more intelligence on potential crisis locations such as Cuba, often in the form of self-explanatory "Radio Propaganda Reports." Special requests were largely in response to existing deficiencies in collection capabilities in areas of special political importance to policymakers. Regarding Cuba, FBIS acknowledged that it was caught off guard when it discovered that "several clandestine radios [i.e. broadcasting stations]" based outside of Cuba were promoting Castro's revolutionary ideals in Guatemala.[192] FBIS likewise lamented that it was unable to receive broadcasts of policy speeches delivered by Castro and another chief minister in December of 1958 in Santiago, Cuba.[193]

FBIS responded to its collection deficiency issues by constructing more monitoring posts between 1957 and 1967. In 1957 FBIS had 10 posts worldwide. A decade later it would add five more, by this year either under construction or

[191] Ibid., 8.
[192] Ibid., 32.
[193] Ibid., 33.

operational.[194] By 1960, most monitoring of Cuba was based out of a post in Puerto Rico. FBIS noted that while this post sufficiently covered Havana and its surrounding area, it did a poor job covering the remainder of the island as well as the rest of Central and South America. By 1966, the construction of two new posts in Key West, Florida as well as Panama sufficiently covered these collection deficiencies.

Lastly, FBIS cited its nebulous identity within the US Intelligence Community as a source of the inefficiencies it sought to correct between 1957 and 1967. Although FBIS was fully integrated into the CIA by 1957, it still perceived an "independent" aspect to its identity due to the high degree of specialization in its activities. FBIS's ambiguous identity caused it to struggle with interagency communication. While FBIS had frequent and expected contact with some components of its CIA overseers, it scarcely had contact with any other agencies in the intelligence community—suggesting that outside the CIA, all source intelligence products underutilized OSINT handled by FBIS. Coupled with the fact that FBIS notes that it was largely in control of who it disseminated its finished intelligence to, it is reasonable to conclude that this implies that interagency intelligence sharing with FBIS was lacking, possibly in all directions.[195]

In summary, between 1957 and 1967, while evidence suggests FBIS was undergoing a period of operational expansion and was gradually increasing its collection capacities, a number of potential sources of collection deficiencies were also noted in the official institutional history. This suggests that an underutilization of OSINT caused by these deficiencies may have contributed to the IC's failure to foresee Soviet deployment of medium-range SS-4 and intermediate-range R-14 ballistic missiles until after they

[194] Ibid., 220.
[195] Ibid., 92.

were deployed to facilities across Cuba. Keep this conclusion in mind as we proceed now to the quantitative experiment itself.

Quantitative Case Study: Cuban Missile Crisis of 1962

A discussion of the background of the intelligence dimensions of the Cuban Missile Crisis and the institutional history of FBIS between 1957 and 1967 could go on indefinitely. With a sufficient number of pages dedicated to outlining the major contextual issues, the thesis can now transition to reporting the results of the case study conducted. Refer to the previous chapter for a reminder of the methodology used to produce the results that follow.

Phase One Results

First, selections from twenty pieces of open source information collected by FBIS between October 16, 1962 and October 28, 1962 were chosen at random. This "raw" OSINT was taken from an online database called the *Foreign Broadcast Information Service (FBIS) Daily Reports*. The word "report" is misleading in this context. The documents one finds using this database are not finished intelligence products, but rather unanalyzed transcripts from a number of speech and radio broadcasts that can be more accurately classified as open source information. Table I below lists the sources that were selected. Note that I, for reference purposes, invented the numbers preceding title names in parentheses.

Table I: FBIS Open Source Information Samples Selected[196]

Source Title	FBIS ID Number	Date of Collection
(1) USSR Offer to U.S. on Cuba Reported	FBIS-FRB-62-203	Oct. 16, 1962
(2) Kiecyle Report	FBIS-FRB-62-209	Oct. 25, 1962
(3) 27 October New York Report	FBIS-FRB-62-211	Oct. 27, 1962
(4) Washington Report	FBIS-FRB-62-210	Oct. 26 1962
(5) Kallai Addresses Cuban Solidarity Rally	FBIS-FRB-62-210	Oct. 25, 1962
(6) Recorded Excerpts	FBIS-FRB-62-210	Oct. 26, 1962
(7) Comment on Security Council Meeting	FBIS-FRB-62-210	Oct. 26, 1962
(8) Wanguemert Comments on Several Topics	FBIS-FRB-62-203	Oct. 17, 1962
(9) Kuchilan Comments on Several Themes	FBIS-FRB-62-206	Oct. 22, 1962
(10) Nesterov Talk to Japan	FBIS-FRB-62-210	Oct. 26, 1962
(11) U.S. Gallup Poll on Cuba	FBIS-FRB-62-205	Oct. 19, 1962
(12) U.N. Emergency Session Discusses Cuba	FBIS-FRB-62-209	Oct. 25, 1962
(13) Matveyev in IZVESTIYA	FBIS-FRB-62-211	Oct. 28, 1962
(14) Kartsev on President's Order	FBIS-FRB-62-208	Oct. 24, 1962
(15) Hinted Cub-W. Berlin 'Deal' U.S. Fraud	FBIS-FRB-62-204	Oct. 18, 1962
(16) David on Policy's Illegality	FBIS-FRB-62-210	Oct. 26, 1962
(17) Underground Tests, Cuba Topics in Geneva	FBIS-FRB-62-208	Oct. 24, 1962
(18) Denial of President's Charges	FBIS-FRB-62-207	Oct. 23, 1962
(19) Shragin on U.S. 'Big Lie'	FBIS-FRB-62-209	Oct. 25, 1962
(20) Review of West German Radio and Press	FBIS-FRB-62-203	Oct. 17, 1962

[196] I also considered an additional, randomly selected 30 pieces of open source information from the aforementioned FBIS database. These additional sources are listed in the bibliography even though they were not directly used in the case study.

Next, ten pieces of finished all-source intelligence with open source elements were selected. These documents were obtained from two online databases, *U.S. Declassified Documents Online* and *CIA Freedom of Information Act Reading Room*, as well as the physical archives of the John F. Kennedy Presidential Library and Museum located in Boston, Massachusetts. As with the raw intelligence, these finished intelligence products were selected randomly, and exclusively between October 16, 1962 and October 28, 1962. I have also numbered sources here for reference purposes. Table II below lists the sources that were selected.

Table II: Finished All-Source Intelligence Products with Open Source Elements Selected[197]

Source Title	Agency	Date of Publication
(1) Joint Evaluation of the Soviet Missile Threat in Cuba	National Photographic Interpretation Center	Oct. 19, 1962
(2) Supplement 8 to Joint Evaluation of Soviet Missile Threat in Cuba	National Photographic Interpretation Center	Oct. 28, 1962
(3) Major Consequences of Certain US Courses of Action on Cuba: SNIE 11-19-62	Central Intelligence Agency	Oct. 20, 1962
(4) Summary Record of NSC Executive Committee Meeting No. 8	National Security Council	Oct. 27, 1962
(5) Summary Record of NSC Executive Committee Meeting No. 7	National Security Council	Oct. 27, 1962
(6) Memorandum for the Record: "Notification of NSC Officials of Intelligence on Missile Bases in Cuba	Department of State	Oct. 27, 1962
(7) Soviet Reactions to Certain US Courses of Action on Cuba: SNIE 11-18-62	Central Intelligence Agency	Oct. 19, 1962
(8) Background Briefing on Cuban Situation	Department of Defense	Oct. 22, 1962

[197] I also considered other randomly selected all-source finished intelligence products of the crisis not utilized in the case study. Refer to the bibliography for more information on those sources.

(9) Memorandum: The Crisis: USSR/Cuba Information as of 0600	Central Intelligence Agency	Oct. 27, 1962
(10) Memorandum: USSR/Cuba	Central Intelligence Agency	Oct. 24, 1962

I then proceeded to objectively evaluate the quality of each piece of raw OSINT and "finished" OSINT (i.e. all-source intelligence with OSINT elements) sampled based on four criteria: (1.) presentability; (2.) accuracy; (3.) actionability; and (4.) objectivity. I based my evaluation of these standards on the following characterizations[198]:

1. *Presentability* refers to the physical appearance of the document. It considers the logical organization of the source as well as its legibility and readability. Presentability takes writing style into account, evaluating to what extent superfluous use of jargon is present. It considers other syntactical and diction matters as well. More presentable sources are easier to follow and read and are more likely to not be skimmed or ignored all together by the layman reader.
2. *Accuracy* refers to the extent to which the information provided by the source can be (1.) deemed objectively truthful and (2.) can be corroborated with other sources. In evaluating both these points, I have referred to the totality of my research on the crisis—with particular focus on corroborating information with two of the most authoritative sources on the minute intelligence details of the crisis: Aleksander Fursenko's *One Hell of a Gamble* and Michael Dobbs's, *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear*

[198] Note that another assumption of the quantitative experiment is that these characteristics of raw and finished intelligence constitute "good" or effective intelligence. A number intelligence studies textbooks have thematically confirmed the importance of this criteria. For two examples see Richard K. Betts, *Enemies of Intelligence*, *supra* n. 34 and Jeffrey T. Richelson, *The U.S. Intelligence Community*, New York: Routledge, 2015.

War.[199]

3. *Actionability* is a measure of to what degree policymakers would be able to use the information provided by a source to make a policy decision. Actionability is not a measure of to what extent a "correct" or "best" decision can be made. It is simply a measure of whether the information provided makes concrete statements and can be utilized to take a future action, regardless of that action's consequences.
4. *Objectivity* refers to the tone of the information being presented. Generally speaking, an objective intelligence document is devoid of hyperbole and emotional language. It avoids stereotyping and equally and fairly presents all angles to a problem or situation, in a professional, journalistic manner. It also avoids preselecting decisions for policymakers, serving as a neutral source of information and taking an erudite tone to its evaluation of the pros and cons of a given situation.

Taking up first the role of a scholar of intelligence, I ranked each piece of raw OSINT and finished OSINT on a scale of one to five in each of these categories, following the above criteria as objectively as possible. After each of these rankings were determined, I then summed the total score in each category for each piece of OSINF or finished OSINT for "Total Quality Points" (TQP), a measure of the overall quality of the intelligence. I also summed and averaged individual scores in each criterion category for a "Quality Points Score" (QPS), an overall assessment of each quality criterion of the two sets of data considered. Tables III and IV summarize the results of these evaluations below.

[199] See supra, nn. 21, 22, 167.

Table III: Raw OSINT Quality Evaluations

ID Number	Presentability	Accuracy	Actionability	Objectivity	TQP
1	3	3	3	4	13
2	3	2	2	3	10
3	3	3	2	3	11
4	3	4	2	4	13
5*	2	2	2	1	7
6	2	2	1	1	7
7	3	4	2	2	11
8*	3	3	2	3	11
9	2	1	1	1	5
10	3	3	2	2	10
11	3	4	2	4	13
12	3	3	4	3	13
13	2	2	3	3	10
14	3	2	3	2	10
15	3	3	3	3	12
16*	2	2	2	1	7
17	3	1	2	2	8
18	3	3	2	2	10
19	3	3	2	3	11
20	3	3	2	4	12
QPS	**2.75**	**2.65**	**2.20**	**2.35**	---

Table IV: Finished OSINT Quality Evaluations

ID Number	Presentability	Accuracy	Actionability	Objectivity	TQP
1	4	4	4	5	17
2	5	4	5	4	18
3*	5	3	3	4	15
4	3	4	3	4	14
5	4	4	3	4	15
6	3	3	3	3	12
7	4	4	3	4	15
8	4	3	3	4	14
9*	4	4	5	5	18
10*	4	4	4	4	16
QPS	**4.40**	**4.10**	**3.60**	**4.10**	---

Note the asterisked sources in the two previous tables. In order to better make sense of how sources were scored on the above-defined measures of quality, it would be useful to elaborate on the scoring rationale behind a select portion of the sampled data. Those randomly selected samples will each be individually discussed.

Table III's source five (3/5) discusses a Budapest report on anti-American protests that took place that day in the Hungarian capital.[200] The report's low scoring on all major quality categories is reflective of the heavily propagandistic nature of the document. The US is entirely depicted as an aggressor, its actions being described as "US aggression", "provocative", and "[in violation] of international law." The "Cuban people" are depicted as a moral force of good: "The people of Cuba want peace." The figure of

[200] Kallai Addresses Cuban Solidarity Rally, FBIS-FRB-62-210, Washington, Oct. 25, 1962.

50,000 Hungarian workers protesting in what was referred to as "Budapest's sports hall" (the Kisstadion) is highly suspect given the arena's maximum holding capacity was only about 17,000 people at the time.[201]

Table III, source eight (3/8) comes from a Havana television broadcast discussing the International Chamber of Navigation's response to the crisis in Cuba and Turkey's relationship with the United States.[202] The source receives higher ratings than 3/5 on accuracy and objectivity for accurately reporting on the trade concerns of the International Chamber of Navigation regarding the potential for a US naval blockade on Cuba.[203] The report falls flatter on actionability, because it only sentimentally ruminates on the general problems of US hostility toward Cuba as well as the dependency of the Turkish government on the United States.

Like 3/5, Table III, source sixteen (3/16) is largely a propaganda piece, ranked of poor quality.[204] Even more so than 3/5, 3/16 utilizes inaccurate hyperbole to describe the US quarantine of Cuba. Coming from a broadcast from Prague, the report is a borderline rant. It calls the US quarantine a "blockade" and an "act of war". It uses the word "smother" to describe US efforts to put down the Cuban Revolution. It also describes US objectives as "shameful" and accuses the US of targeting the people of Cuba directly in its acts of sabotage –accusing the US of desiring to "shell" civilians.

The propagandistic nature of these three raw intelligence samples does not render this OSINF totally devoid of intelligence value. However, extremely biased OSINF

[201] "Kisstadion," Hungarian Ministry of Human Resources, https://www.kulturinfo.hu (accessed April 19, 2019).
[202] Wanguemert Comments on Several Topics, FBIS-FRB-62-203, Washington, Oct. 17, 1962.
[203] Turki Althunayan, *Dealing with the Fragmented International Legal Environment: WTO, International Tax and Internal Tax Regulations*, New York: Springer, 2010, 95-98.
[204] David on Policy's Illegality, FBIS-FRB-62-210, Washington, Oct. 26, 1962.

making liberal use of false statements and exaggeration is inherently much less valuable to policymakers than intelligence that presentably provides accurate, actionable, and objective information. I turn now to the finished OSINT.

Table IV, Source three (4/3) is a CIA produced Special National Intelligence Estimate (SNIE) (dated October 20) on possible decisions to be made on the Cuban Missile Crisis.[205] The finished intelligence product receives a perfect score on presentability, for the logical and clear manner in which potential policy options are organized. The document is not superfluously wordy or technical and consequently is readable for a policymaker perhaps not completely familiar the terminology of missile technologies. While the source could be clearer on the policy recommendations it specifically delineates as options, overall the document provides an accurate and objective assessment of the crisis by that stage.

Like 4/3, Table IV, source nine (4/9) scores highly on quality, especially on actionability and objectivity.[206] The document makes astute psychological observations, noting in one speech that Castro delivered "that…[he] seemed tired and uncertain at the beginning of the speech and his audience of government and party leaders looked serious and even glum".[207] The report also accurately takes note of the progress of 16 Soviet dry cargo ships with military supplies en route to Cuba, going as far to predicting specific times in which two of the freighters would be expected to reach Havana harbor.[208] The source also presents itself well by touching on a broad range of issues related to the crisis

[205] Major Consequences of Certain US Courses of Action on Cuba, SNIE 11-19-62, Washington, Oct. 20, 1962.
[206] Memorandum for the Record: "Notification of NSC Officials of Intelligence on Missile Bases in Cuba", Cline, Washington, Oct. 27, 1962.
[207] 23rd of October Speech, Latin American Network Information Center: Castro Speech Database, San Paolo, October 23, 1962.
[208] Dobbs, *One Minute to Midnight*, 180.

at the time, even assessing the messages coming out of communist bloc propaganda networks in Eastern Europe.

Table IV, source ten (4/10), like 4/9 and 4/3, scores highly on quality.[209] This source –a CIA memorandum on the general development of the crisis (dated October 24) –is commendable in part for its accurate list of nine ships that recently docked in various parts of Cuba over the past few days, before it was written.[210] The source also provides a very actionable list of diplomatic responses to the crisis to date from governments around the world, ranging from statements from West Germany's chancellor to government propaganda broadcasts from Algeria.[211]

Phase Two Results

To assess the quantity aspect of the relationship between OSINT and national security decision-making, Phase Two of the case study experiment began with the creation of a list of ten possible (and realistic) national security policy decisions the Kennedy Administration could have made throughout the crisis, with *potential* outcomes for these decisions accompanying each choice. Table V below lists these policy decisions and their respective outcomes.

[209] The Crisis: USSR/Cuba, CIA Memorandum, Washington, Oct. 24, 1962.
[210] Dobbs, *One Minute to Midnight*, 180-81.
[211] Ibid., 163-170.

Table V: Ten Cuban Missile Crisis Hypothetical National Security Decisions and Potential Outcomes

Possible Decision	Potential Outcome
Option 1: US forces launch a full scale invasion of Cuba (land, naval, air)	Soviets use tactical nuclear missiles to repel invasion; these missiles also used in offensive attack against US forces stationed in Guantanamo Bay naval base
Option 2: US navy and air force commence airstrikes against missile sites in Cuba; airstrikes *alone* are conducted (SAM, SS-4, and R-14 sites)	Soviet forces retaliate against US forces stationed in Guantanamo Bay base; utilization of tactical nuclear missiles included in counterattack
Option 3: US naval forces impose a sea-based quarantine of Cuba; US forces not allowed to engage Soviet commercial and/or military ships under any circumstances without direct approval from Washington	Soviet commercial and/or military ships effectively deterred by presence of quarantine; all ships en route to Cuba cease their present course, are diverted to non-Cuban ports/return to their port of departure
Option 4: The US does not militarily respond to the crisis; diplomatic efforts to find a favorable outcome are minimal/tepid	Soviets complete construction of all intended SS-4 and R-14 ballistic missiles sites in Cuba; all sites in due time are rendered fully operational
Option 5: US naval forces impose a sea-based quarantine of Cuba; US forces allowed to engage Soviet commercial and/or military ships without direct approval from Washington	Soviet ship with military cargo for missile site construction sunk by US naval forces after ship fails to stop at quarantine line; nearby Soviet submarine with nuclear tipped missiles strikes US carrier group in retaliation, absent orders from Moscow
Option 6: US President authorizes CIA to conduct covert sabotage operations targeting Cuban critical infrastructure	Soviets do not militarily respond to successful acts of sabotage but signs pointing to US authorization of the attacks significantly escalates diplomatic tensions; Castro regime given greater leeway to authorize use of Soviet military equipment on the island for defensive purposes
Option 7: Kennedy authorizes CIA to conduct a covert operation to assassinate Fidel Castro	Assassination attempt fails; Soviet and Cuban intelligence points to US involvement; diplomatic tensions significantly escalate; Castro regime given greater leeway to authorize use of Soviet military equipment on the island for defensive purposes
Option 8: US anticipates Soviet invasion of West Germany from East Germany; US military attention primarily directed to deterring Soviet threat to West Germany	US military buildup in West Germany deters both Soviet invasion of West Germany from East Germany and Soviet escalation of military tensions over Cuba; Soviets impose moratorium on missile site construction in Cuba
Option 9: US withdraws a significant portion of its military presence from West Germany to deescalate tensions; US military focus shifts to deterring Soviet missile site construction in Cuba	Soviets take advantage of West Germany military pull out and seize West Berlin; Soviets stop short of invading the rest of West Germany; US and its allies do not use nuclear weapons against the Soviet Union or any of its satellite states
Option 10[212]: US does not militarily respond to the	Missile site construction in Cuba continues while

[212] Note that Option 10 will be the DR option (i.e. the *optimal policy result*) of the experiment as its outcome most meets the policy objectives of the Kennedy Administration during the crisis (i.e. completely removing the missiles from Cuba and avoiding a thermonuclear exchange with the Soviet Union). For more on the policy objectives of the Kennedy Administration during the crisis confirming this view see Michael H. Hunt, *Crises in U.S. Foreign Policy: An International History Reader*, New Haven: Yale University

crisis but focuses its attention on reaching a diplomatic settlement	negotiations are ongoing but diplomatic settlement reached; US promise not to invade Cuba and to withdraw Jupiter missiles from Turkey in exchange for Soviet deconstruction of missile sites in Cuba

I then begin three rounds of using the sampled raw and finished intelligence from Phase One to individually determine, as a layman policymaker, which of the ten potential options (if any) each piece of intelligence would most support making. Note that intelligence sampled could be ruled to support multiple national security decision-making options. Also remember that in each round of the experiment more intelligence was randomly added to determine whether or not a greater quantity of intelligence improves collection capabilities. Intelligence from the previous round was *added* to intelligence of the subsequent round in determining the DX option for each round after the first. Recall also that one of the primary operating assumptions of this experiment, based on the theoretical conclusions of Part One of the thesis, is that intelligence in general has at least some impact on which decisions are made in a national security context. Lastly, note that an "X" listed below signifies that that the source supports none of the ten listed national security decision-making options. Tables VI and VII below summarize the results of Phase Two.

Press, 1996, and *supra* n. 6. I assume that of the ten listed options, US policymakers of the Kennedy Administration would have most favored this outcome, because it both avoids a military confrontation and is the only option outcome in which missile site construction not only ceases, but missiles are removed from Cuba altogether.

Table VI: Phase Two, Raw OSINT

---	ID Number	Supporting Options
ROUND ONE	1	8
---	4	10
---	12	4, 10, 6, 7, 9
---	17	10, 4
---	20	10, 8
ROUND ONE DX	---	**10**
ROUND TWO	2	9, 1, 2
---	3	9, 10, 4
---	6	4, 2, 3, 5
---	7	3, 4, 10
---	19	4, 10
---	18	3, 5, 2
---	15	10, 8, 9
---	14	3, 5, 4, 1
---	13	9, 10, 1, 2, 5
---	10	10, 4
ROUND TWO DX	---	**10**
ROUND THREE	9	6, 7, 1, 2
---	11	10, 4
---	16	3, 5, 6, 7
---	8	1, 2, 4, 5, 10
---	5	10
ROUND THREE DX	---	**10**

Table VII: Phase Two, Finished OSINT

---	ID Number	Supporting Options
ROUND ONE	2	2
---	6	X
---	7	8, 10, 9
ROUND ONE DX	---	**Inconclusive**
ROUND TWO	1	2, 3, 5
---	8	3, 5, 10
---	10	10, 3, 5, 1
---	9	3, 5, 10
---	4	10, 1, 2
ROUND TWO DX	---	**10**
ROUND THREE	3	8, 1, 2
---	5	10, 8
ROUND THREE DX	---	**10**

Lastly, to complete the testing of the experimental nexus between quality of OSINT sampled and quantity of OSINT sampled, I calculated the Total Quality Points for each of the six rounds of Phase Two of the case study (using the TQPs calculated for each individual source in Phase One, all of which summed together for a round by round TQP). Note that the round-by-round TQP quantities are not the cumulative quantity of TQP (from previous rounds) but simply the quantity of quality points *added* by the round. The results of these calculations are summarized in Table VIII below.

Table VIII: Round by Round TQPs for Phase Two

Table (VI or VII)	Round	Total Quality Points (TQP)
VI	1	+59
VI	2	+105
VI	3	+43
VII	1	+45
VII	2	+79
VII	3	+30

To begin making sense of these numbers, a similar exercise to that conducted at the end of Phase One of the experiment is useful for understanding how intelligence source were determined to "connect" to individual national security decisions. Before one can begin to reapply this exercise, a description of the standard use to construct potential connections is first necessary.

The standard looks exclusively at the *actionability* of the intelligence source. I essentially asked myself the following with each source: *What are the policy implications of this intelligence? If I were in the Kennedy Administration and this intelligence source made its way to my desk, how would I interpret it? Which options are encouraged either explicitly or implicitly? Which options are discouraged either implicitly or explicitly? What would I advise as a policymaker to my EXCOMM colleagues and/or superiors?*[213]

[213] A potential issue with this assumption is that of outcome bias, or an error made in evaluating the quality of a decision when the outcome of that decision is already known. A solution to this problem may involve having an individual completely unfamiliar with the historical outcome of the Cuban Missile Crisis (perhaps not impossible to find in today's world) participate in the quantitative case study experiment. For more on bias outcomes see Nidhi Agrawal and Durairaj Maheswaran, "Motivated Reasoning in Outcome-Bias Effects", *Journal of Consumer Research* 31, no. 4 (2005): 798-805.

Highly actionable sources are more likely to encourage specific policy decisions than less actionable sources. Policy decisions encouraged or discouraged do not necessarily need to be explicit –they can be implied as well. Options encouraged or discouraged do not necessarily need to be consistent with one another either. The oftentimes inherently ambiguous nature of intelligence sources does not preclude rational but conflicting interpretations from being deduced as realistic possibilities of actions.

Beginning with the raw OSINT, consider Table VI, source 17 (6/17), a source from the Soviet Union's state-run media service TASS.[214] The source discusses in part Soviet reception toward President Kennedy's October 22 speech announcing the naval quarantine of Cuba. The Soviet source refers to the US move in ominous terms, describing it as "a threat to universal peace" or a movement "toward the precipice of war." The implication that what was effectively a naval blockade might lead to a conflict between Soviet and US military forces on international waters likely had a deterrent effect, signaling a degree of Soviet military resolve toward challenging the blockade. The resultant effect likely would have inclined the policymaker more in the direction of a nonmilitary response to the crisis.

Table VI, source 15 (6/15) discusses the Cuba-West Berlin nexus that preoccupied policymakers from both side of the crisis.[215] Another Moscow based state media source, the source suggests that as long as the US "eases its attitude" over West Berlin, the Soviet Union will pursue a more moderate course of action over Cuba. While the source's hinting of military conflict generally suggests diplomacy as the best alternative to a confrontation, the source offers conflicting suggestions relating to Berlin.

[214] Underground Tests, Cuba Topics in Geneva, FBIS-FRB-62-208, Washington, Oct. 24, 1962.
[215] Hinted Cub-W. Berlin 'Deal' U.S. Fraud, FBIS-FRB-62-204, Washington, Oct. 18, 1962.

The Soviets may have been encouraging US military concessions in West Germany for the express purpose of strengthening the Soviet hand in West Germany or out of a genuine self-defensive fear of the security of East Germany. In other words, the policymaker could rationally make arguments that this intelligence source either supports or does not support more US military attention devoted to the security of West Germany.

Table VI, source nine (6/9) is an October 19 report from state-controlled Havana television network discussing the proliferation of Cuban exiles or "traitors" under US asylum in places like Florida, Puerto Rico, and Panama.[216] The report goes on to discuss the security threat these exiles pose to Cuba. The source suggests either a legitimate Cuban fear of these refugees outside of Cuba or an effort by the Cuban government to stoke fears of another attempt by the US to intervene in the affairs of Cuba using an expatriate force (i.e. another Bay of Pigs situation or another attempt at taking Fidel Castro's life). A policymaker could take two angles to analyzing this source. The first may suggest that any attempt to mobilize the Cuban people in a concerted effort against Castro would fail and therefore more direct military action would be the better option. The other view suggests a kind of reverse psychology approach to the situation (assuming the Cubans see the expatriate threat as a legitimate threat): since the Cuban government expects an intervention involving expatriates and has made their expectation public, they would assume that the US would not go as far to intervene using expatriates in any future effort; therefore the best option for US forces would be to intervene with expatriates to catch the Cuban government off guard.

Turning to the finished OSINT now, Table VII, source three (7/3) –a supplement to a report written by the National Photographic Interpretation Center, is difficult to

[216] U.S. Gallup Poll on Cuba, FBIS-FRB-62-205, Washington, Oct. 19, 1962.

assess on policy recommendations as the report explicitly acknowledges, "This report does not attempt to estimate Soviet attempt to attack the United States."[217] The report's very detailed description of the missile sites and appraisals suggesting that the sites are largely operational hints that a forceful solution would be the best means of disabling the sites and interrupting the construction process. However, generally speaking, the source is very neutral in tone and makes no concrete national security policy recommendations.

Similar to 7/3, Table VII, source six (7/6) also lacks in pointing to a specific policy option, but even more so.[218] This State Department memorandum only discusses an unsubstantiated rumor that a general deliberately withheld U-2 intelligence on the construction of the missile sites from President Kennedy. While a political scientist may find value to this memorandum, from an intelligence perspective relating to national security decision-making, it largely does not relate to the crisis itself and therefore does not merit being classified as suggesting a policy response.

Lastly, Table VII, source one, like 7/3, comes from an assessment of the crisis from the National Photographic Interpretation Center discussing evidence of the construction of the missile sites, with a focus on the movement of missile supplies on Soviet freighters. Considering potential Cuban ports that these ships would likely travel to in an effort to offload their cargoes, as well as providing a detailed discussion on the construction progress of the sites (e.g. special security fences and potential tactical nuclear missile movements), suggests that the policymaker considering this intelligence

[217] Supplement 8 to Joint Evaluation of Soviet Missile Threat in Cuba. Guided Missile and Astronautics Intelligence Committee, Joint Atomic Energy Intelligence Committee, National Photographic Interpretation Center, Washington, Oct. 28, 1962.
[218] Memorandum for the Record: "Notification of NSC Officials of Intelligence on Missile Bases in Cuba". Cline, Washington, Oct. 27, 1962.

source would likely see potential in a military solution to the crisis, particularly a naval one.

With these results of the case study experiment now fully reported, this concludes this chapter on the Cuban Missile Crisis of 1962. To review, this chapter attempted to introduce the historical context in which the OSINT and national security decision-making variable were present during the crisis. The chapter then proceeded to walk the reader through the quantitative test employed to test the two research questions of Part Two. The final chapter of the thesis will analyze and interpret these quantitative results and also offer some final, concluding remarks on the overall question of the nexus (or lack thereof) between Open Source Intelligence and national security decision-making.

CONCLUSION

This final, concluding chapter of the thesis begins with a discussion of the meaning behind the results of the case study reported in the previous chapter, answering the research questions Part Two of the thesis posed in the process of doing so. The chapter will then discuss the potential for future case studies, based on the foundation laid by the empirical test methodology the case study employed. The chapter concludes with a final statement on the possible nexus between the OSINT variable and the national security decision-making variable, returning in part to the conclusions related at the end of Part One.

Experiment Results: Analysis and Conclusions

Part One of the paper has concluded that there is likely, at least in theory, some causal connection between the OSINT variable and the national security decision-making variable, even if determining the specifics of that causal connection is presently impossible. Part Two sought to clarify this relationship by assessing whether OSINT contributes to decision-making leading to more optimal policy results.

On the case study issues of quantity and quality, Tables III and IV suggest that between finished OSINT products and unfinished OSINT products, finished OSINT products are all-around higher in quality (assuming a "high" quality product is more or less measured by greater presentability, greater accuracy, greater actionability, and greater objectivity). The difference in Quality Points Score (QPS) between Tables III and IV suggests this is so, and that on average, the quality of finished OSINT products is

about double that of unfinished OSINT products. This conclusion is very sensible given that finished OSINT products are inherently more refined versions of their "raw" OSINT product predecessors. Considering the theoretical flow of the intelligence cycle, the former undergo the complete process of the intelligence cycle, whereas the latter are produced solely by the collection phase of the cycle and do not receive further refinement.[219]

An initial consideration of Tables VI and VII of the experiment may suggest that increases in the quantity of OSINT products has no impact on national security decision-making given that for all six rounds of Phase Two of the experiment, the intelligence products considered report that the "decision-made" (DX) falls in line with the historical decision (DR or Option 10). However, a closer look at the data reveals that while DR = DX for every round of Phase Two, there is evidence to sustain that the *margin* by which the DX remains Option 10 increases as quantity of OSINT products increases, at least for unfinished OSINT products. In Table VI, Round One, Option 10 (x4 selections) defeats runner-up Option 4 (x2 selections) by a margin of two. In Round Two, Option 10 (x10 selections total) defeats runner-up Option 4 (x6 selections total) by a margin of four. Lastly, Round Three Option 10 (x13 selections total) defeats runner-up Option 4 (x8 selections total) by margin of five. This data suggests that as quantity of raw OSINT products increases, the *certainty* by which Option 10 is selected as the DX increases.

This same trend appears with the finished intelligence products, but less

[219] It is important to note that, as Chapter Four established, policymakers receive information they use to make national security decisions not exclusively from the formal structures of national security decision-making, like from the IC-NSC nexus. Policymakers also receive information from informal structures like advisory systems. Likewise, while policymakers receive finished intelligence products from formal structures, nothing prevents them from seeking "unrefined" or "raw" OSINF directly and making decisions based on this unprocessed OSINF alone. This realty is the reason why the quantitative test considered not only finished OSINT products' impact on national security decision-making, but OSINF's as well.

evidently, and consequentially less conclusively. Table VII, Round One's results are inconclusive, with no DX winner able to be chosen given the four way tie of options between Options 2, 8, 9, and 10 (one can consider this outcome the farthest from the DR). In Round Two, Option 10 emerges as the DX (x5 selections total), but only defeats runner-up Option Five (x4 selections total) by a margin of one. In Round Three, this margin of victory increases but only by one, with Option 10 (x6 selections total) defeating runner-up Option Five (x4 selections total).

On the question of increasing quality, again the evidence suggests that increasingly quality leads to national security decision-making that produces more optimal policy results, but somewhat unclearly. Considering the Total Quality Points (TQP) values calculated in Table VIII, it can be noted that the margin by which the certainty that Option 10 is the DX doubles between Round One and Round Two. This can be compared to the about doubling of TQP added between these two rounds, suggesting that a doubling of quality led to a doubling of certainty. An identical trend of doubling can also be noted between rounds One and Two of Phase Two's consideration of finished OSINT products. However, despite this "doubling" trend noted twice in the experiment, no other trends of increasing TQP between rounds leading to a corresponding increase in certainty can be noted. Therefore, it is appropriate to render the judgment that the results on quality increases are largely inconclusive.

This consequentially means that the quantitative evidence suggests that increasing quantity of unfinished OSINT products *may* contribute to national security decision-making that produces more optimal policy results. However, the inconclusive nature of the answer to the question of increasing quality producing these results means assessing

an increase in both variables simultaneously is not possible. Therefore, the answer to the question of both increases in quantity and quality of OSINT intelligence products remains overall inconclusive.

Future Studies

The methodology employed in this thesis for the case study experiment could be modified in a plethora of ways. These modifications could be most evidently employed in the core assumptions adopted in conducting the experiment. For example, the criteria for assessing quality of an intelligence product (presentablity, accuracy, actionability, and objectivity) could be modified both definitionally and regarding which criteria categories are selected. Other quality criteria options could include *timeliness* (i.e. the timing context in which the intelligence product is produced), *visibility* (i.e. who has access to the intelligence document), or *confidence* (i.e. the tone of certainty that the intelligence product exudes). The assumption that the DR, while grounded in part by the historical reality of the decisions made during the Cuban Missile Crisis, could be modified to include other possible outcomes. Historians, political scientists, and scholars of international relations are far from being in total agreement on what was or could have been the "best" outcome of the crisis or even what a "best" or optimal outcome means.

The study could be structurally altered as well. Such a modification could include choosing another historical episode. Indeed, I strongly recommend that future scholars interested in the questions this thesis asks to alter the experimental methodology to include other historical scenarios where OSINT has been documented to have played a notable role in intelligence: such as the surprise Japanese attack on Pearl Harbor, the

Sino-Soviet split, and the Chinese invasion of North Vietnam.[220] Of course the range of historical episodes that could be utilized will depend on what intelligence is declassified by the US Intelligence Community and when.

In summary, the methodology employed in Part Two of this thesis could be improved or experimented with in a variety of ways. I strongly encourage readers and scholars interested in the principle research questions addressed to devote future energies to quantitative studies on OSINT to clarify uncertainties discussed in this thesis.

Additionally, the relatively novel nature of Second Generation OSINT (coupled with signs of an emerging Third Generation) presents an evident need for greater information on the relationship between the variables of OSINT and national security decision-making. OSINT, especially if a third generation comes into being, could revolutionize the way in which the United States produces intelligence for policymakers tasked with making national security decisions. In order to accurately assess to what extent resources devoted to improving OSINT capabilities should be allocated, policymakers will need to determine to what extent the OSINT discipline actually contributes to more informed national security decision-making.

Final Remarks

To recall, it was concluded at the end of Chapter Five that theoretically, OSINT that successfully collects and filters OSINF and produces timely, accurate, and objective finished OSINT products and is received by policymakers through the formal and informal structures of national security decision-making will generally contribute to

[220] For a list of even more historical events in which intelligence and national security scholars alike have reason to believe OSINT notably impacted national security decision-making see Mercado, "Sailing the Sea of OSINT in the Information Age," 'Navigating Cold War Waters' & 'OSINT, OSINT, everywhere…'

more-informed national security decision-making, which in turn will produce more optimal policy results.

Now while Part One of the thesis's exploration of the theoretical relationship between the OSINT variable and the national security decision-making variable suggests that there exists a broad relationship between the two, a quantitative analysis of increases in the quality and quantity of OSINT products casts doubt in part on whether the decisions that are influenced by OSINT produce optimal policy outcomes. Nonetheless, there is reason to conclude that finished OSINT products have greater quality value than unfinished OSINT products or "raw" open source information. There is also reason to believe that increases in quantity of unfinished OSINT (i.e. voluminous collection) may lead to greater certainty in national security decision-making that will produce more optimal policy outcomes. The data however also suggest that the question of whether the sheer quantity of OSINT (i.e. finished and unfinished combined) has a causal relationship with national security decision-making that produces optimal policy results remains unresolved. Lastly, the data suggests that the question on increases in quality as well as increases in quantity and quality simultaneously is also inconclusive.

The partially inconclusive answers to the research questions of this thesis does not merit reason to believe that more conclusive answers will never be drawn in future research on these issues. A consideration of a greater quantity and variety of data, as well as perhaps other methodological modifications, may lead to more conclusive answers in future studies concerning the questions this thesis poses.

In any case, the Open Source Intelligence discipline rightfully deserves the attention of political scientists, scholars of international relations, and scholars of

intelligence studies. This thesis began by mentioning the emergence of an "open source revolution." The technological gears of history will continue to turn, regardless of what scholars of intelligence and national security conclude about OSINT's theoretical or practical value. I hope that the countless hours of research and experimenting used to produce what has been hereto put to paper will encourage future scholars to continue exploring the potential value of Open Source Intelligence.

BIBLIOGRAPHY

Books

Aldrich, Richard J., Rory Cormac, and Michael S. Goodman. *Spying on the World: The Declassified Documents of the Joint Intelligence Committee, 1936-2013.* Edinburgh: Edinburgh University Press, 2014.

Allison, Graham. *Essence of Decision: Explaining the Cuban Missile Crisis*. New York: HarperCollins, 1971.

Althunayan, Turki. *Dealing with the Fragmented International Legal Environment*: *WTO, International Tax and Internal Tax Regulations*. New York: Springer, 2010, 95-98.

Atwan, Abdel Bari. *After bin Laden: Al Qaeda, the Next Generation*. New York: The New Press, 2013.

Asaad, Al-Saleh. *Voices of the Arab Spring: Personal Stories from the Arab Revolutions*. New York: Columbia University Press, 2015.

Benson, Leslie. *Yugoslavia: A Concise History*. London: Palgrave Macmillan, 2003.

Betts, Richard K. *Cruise Missiles: Technology, Strategy, Politics*. New York: Brookings Institution Press, 1981.

Betts, Richard K. *Enemies of Intelligence: Knowledge and Power in American National Security.* New York: Columbia University Press, 2007.

Blight, James G., ed. and David A. Welch, ed. *Intelligence and the Cuban Missile Crisis*. New York: Routledge, 1998.

Block, Fred, and Mathew R. Keller. *State of Innovation: The US Government's Role in Technology*, New York: Routledge, 2011.

Bowden, Mark. *Black Hawk Down: A Story of Modern War*. New York: Grove Press, 2010.

Braybrooke, David, and Charles E. Lindblom. *A Strategy of Decision*. New York: Free Press, 1963.

Burke, John P. *Honest Broker?: The National Security Advisor and Presidential Decision Making*. College Station: Texas A&M University Press, 2009.

Chandler, Alfred. *Strategy and Structure*, Cambridge: MIT Press, 1962.

Chang, Jung, and Jon Halliday. *Mao: The Unknown Story*. New York: Anchor Press, 2006.

Clark, Wesley K. *Winning Modern Wars: Iraq, Terrorism and the American Empire*. Washington: PublicAffairs, 2004.

Dobbs, Michael. *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War*. Visalia: Vintage Press, 2009.

Dyson, Tom, ed., et al. *Precision Strike Warfare and International Intervention: Strategic, Ethico-Legal and Decisional Implications, First Edition.* New York: Routledge, 2015.

Eisenhower, Dwight D. *Waging Peace*, Garden City: Doubleday, 1965.

Friedberg, Aaron L. *A Contest for Supremacy: China, America, and the Struggle for Mastery in Asia*. New York: W.W. Norton and Company, 2012.

Fursenko, Aleksander. *One Hell of a Gamble: Khrushchev, Castro, and Kennedy, 1958-1964: The Secret History of the Cuban Missile Crisis*. New York: W.W. Norton &

Company, 1998.

George, Alexander L. *Presidential decision-making in foreign policy*. Boulder: Westview Press, 1980.

Gilbert, Martin. *Israel: A History*. New York: Harper Perennial, 2008.

Green, James R. *The International Court of Justice and Self-Defense in International Law*. London: Bloomsbury Publishing, 2009.

Haas, Mark L. *The Arab Spring: Change and Resistance in the Middle East*. Boulder: Westview Press, 2012.

Hanhimäki, Jussi M. *The United Nations: A Very Short Introduction*. New York: Oxford University Press, 2008.

Hunt, Michael H. *Crises in U.S. Foreign Policy: An International History Reader*. New Haven: Yale University Press, 1996.

Jablonsky, David et al. *U.S. National Security: Beyond the Cold War*. Carlisle: U.S. Army War College Strategic Studies Institute Press, 1997.

Janis, Irving. *Groupthink: psychological studies of policy decisions and fiascoes*. Boston: Houghton Mifflin, 1982.

Jarmon, Jack A. *The New Era in U.S. National Security: An Introduction to Emerging Threats and Challenges*. Lanham: Rowman & Littlefield Publishers, 2014.

Jervis, Robert. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca: Cornell University Press, 2010.

Johnson, Dominic. *Failing to Win: Perceptions of Victory and Defeat in International Politics*. Cambridge: Harvard University Press, 2006.

Johnson, Loch K, ed. *Handbook of Intelligence Studies*. New York: Routledge, 2006.

Johnson, Richard T. *Managing the White House*, New York: Harper and Row, 1974.

Johnson, Rob. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Collingdale: DIANE Publishing Company, 2005.

Katselli, Elena. *The Problem of Enforcement in International Law: Countermeasures, the Non-Injured State and the Idea of International Community*. New York: Routledge, 2011.

Krebs, Ronald R. *Narrative and the Making of US National Security*. New York: Cambridge University Press, 2015.

Kugler, Richard. *New Directions in U.S. National Security Strategy, Defense Plans, and Diplomacy*. Washington: National Defense University Press, 2011.

Lister, Charles. *The Syrian Jihad: Al-Qaeda, the Islamic State and the Evolution of an Insurgency, First Edition*. New York: Oxford University Press, 2016.

Lord, Carnes. *The Presidency and the Management of National Security*. New York: Free Press, 1988.

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

MacNeil, Neil. *The American Senate: An Insider's History*. New York: Oxford University Press, 2015.

Maddrell, Paul, ed. *The Image of the Enemy: Intelligence Analysis of Adversaries since 1945.* Washington: Georgetown University Press, 2015.

Manchester, William. *American Caesar: Douglas MacArthur 1880-1964*. Boston: Back Bay Books, 2008.

Mansell, Wade. *International Law: A Critical Introduction*. London, Bloomsbury

Publishing, 2013.

March, James G. *A Primer on Decision Making*, New York: Free Press, 1994.

Miller, Paul D. *American Power and Liberal Order*. Washington: Georgetown University Press, 2016.

Moore, Harold G. *We Were Soldiers Once…and Young: Ia Drang—the Battle that Changed the War in Vietnam*. New York: Presidio Press, 2004.

Mousavian, Seyed Hossein. *Resolving the Iran-US Conflict: An Authoritative View From Tehran*. London: Bloomsbury Publishing, 2015.

Nickerson, Jackson, and Ronald Sanders. *Tackling Wicked Government Problems: A Practical Guide for Developing Enterprise Leaders*. Washington: Brookings Institution Press, 2014.

Odom, William E. *Fixing Intelligence: For a More Secure America*. New Haven: Yale University Press, 2003.

Park, Kyung-Ae, ed. *Non-Traditional Security Issues in North Korea*. Honolulu: University of Hawai'i Press, 2013.

Pfaltzgraff, Robert L. Jr, and Uri Ra'anan. *National Security Policy: The Decision-making Process*. Hamden: Archon Books, 1984.

Porter, Roger. *Presidential decision-making: The economic policy board*. New York: Cambridge University Press, 1980.

Rhodes, Christopher J. *The Use of Open Source Intelligence in the Construction of Covert Social Networks*, Vienna: Springer, 2011.

Sechser, Todd S. *Nuclear Weapons and Coercive Diplomacy*. Cambridge: Cambridge University Press, 2017.

Schaub, Gary Jr., ed., and Ryan Kelty, ed. *Private Military and Security Contractors: Controlling the Corporate Warrior*. Lanham: Rowman & Littlefield Publishers, 2016.

Schelling, Thomas C. *Arms and Influence*. New Haven: Yale University Press, 1966.

Schelling, Thomas C. *The Strategy of Conflict*. New Haven: Yale University Press, 1980.

Simon, Herbert A. *Administrative Behavior: A Study of Decision-Making Process in Administrative Organizations*. New York: Free Press, 1945.

Smith, Curt. *George H.W. Bush: Character at the Core*. Lincoln: University of Nebraska Press, Potomac Books, 2014, 158-190.

Stewart, Brian T.W., Samantha Newbery. *Why Spy? The Art of Intelligence, First Edition*. New York: Hurst, 2015.

Synder, Glen. *Deterrence and Defense*, Princeton: Princeton University Press, 1961.

Dijck, José van. *The Culture of Connectivity: A Critical History of Social Media*. New York: Oxford University Press, 2013.

Walcott, Charles E. and Karen M. Holt, *Governing the White House,* Lawrence: University Press of Kansas, 1995.

Watson, Cynthia. *US National Security: A Reference Handbook, Second Edition*. Santa Barbara: ABC-CLIO, 2008.

Westerfield, H. Bradford. *Inside the CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992.* New Haven: Yale University Press, 1995.

Weiss, Linda. *The National Security State and Technology Leadership*. Ithaca: Cornell University Press, 2014.

Wiil, Uffe Kock, ed. *Counterterrorism and Open Source Intelligence: Models, Tools,*

Techniques, and Case Studies. New York: Springer-Verlag Wien, 2011.

Williamson, Myra. *Terrorism and International Law: The Legality of the Use of Force Against Afghanistan in 2001*. Farnham: Ashgate, 2009.

Worley, D. Robert. *Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System*. Lincoln: University of Nebraska Press, 2015.

Zenko, Micah. *Between Threats and War: U.S. Discrete Military Operations in the Post-Cold War World, First Edition*. Stanford: Stanford Security Studies Press, 2010.

Conference Papers and Presentations

Appiah-Kubi, Kojo. "Policy Making Process." PowerPoint. DRUSSA-ISSER Executive Training on 'Influencing Policy.' December 10, 2015, slides 2/32., 11/32.

Mocanu, Mircea. "Open Source Exploitation and the Concepts of Knowledge Development/Understanding". Paper presented at the International Scientific Conference Strategies XXI: the Complex and Dynamic Nature of the Security Environment, Bucharest, Romania, November 22-23, 2012.

Grigorescu, Razvan. "The Role of OSINT In Achieving and Maintaining Security." Paper presented at the International Scientific Conference Strategies XXI: the Complex and Dynamic Nature of the Security Environment, Bucharest, Romania, November 22-23, 2012.

Intelligence

27 October New York Report. FBIS-FRB-62-211. Washington, Oct. 27, 1962.

Alekseyev on Cuba, Germany. FBIS-FRB-62-209. Washington, Oct. 25, 1962.

Background Briefing on Cuban Situation. The Pentagon. Washington, Oct. 22, 1962.

Baturin on 'Defensive' Arms. FBIS-FRB-62-209. Washington, Oct. 24, 1962.

23rd of October Speech. Latin American Network Information Center: Castro Speech Database. Rio de Janeiro, October 23, 1962.

Comment on Security Council Meeting. FBIS-FRB-62-210. Washington, Oct. 26, 1962.

David on Policy's Illegality. FBIS-FRB-62-210. Washington, Oct. 26, 1962.

Denial of President's Charges. FBIS-FRB-62-207. Washington, Oct. 23, 1962.

Department of State Telegram: DIA to Secretary of State. Washington, Oct. 23, 1962.

Domestic News Commentary. FBIS-FRB-62-209. Washington, Oct. 25, 1962.

Domestic News Commentary. FBIS-FRB-62-210. Washington, Oct. 26, 1962.

Executive Committee Record of Action. EXCOM No. 4. Washington, Oct. 25, 1962.

Golikov on Cuban Impressions. FBIS-FRB-62-209. Washington, Oct. 25, 1962.

Government Statement on Cuban Crisis. FBIS-FRB-62-209, Washington, Oct. 25, 1962.

Hinted Cub-W. Berlin 'Deal' U.S. Fraud. FBIS-FRB-62-204, Washington, Oct. 18, 1962.

Fidel Castro's 23 October Interview. FBIS-FRB-62-208, Washington, Oct. 24, 1962.

Joint Evaluation of the Soviet Missile Threat in Cuba. Guided Missile and Astronautics Intelligence Committee: Joint Atomic Energy Intelligence Committee: National Photographic Interpretation Center. Washington, Oct. 19, 1962.

Kallai Addresses Cuban Solidarity Rally. FBIS-FRB-62-210. Washington, Oct. 25, 1962.

Kartsev on President's Order. FBIS-FRB-62-208. Washington, Oct. 24, 1962.

Kiecyle Report. FBIS-FRB-62-209. Washington, Oct. 25, 1962.

Khrushchev Telegram to Thant 27 October. FBIS-FRB-62-211. Washington, Oct. 29, 1962.

Kuchilan Comments on Several Themes. FBIS-FRB-62-206. Washington, Oct. 22, 1962.

Kudryavtsev in RED STAR. FBIS-FRB-62-203. Washington, Oct. 16, 1962.

Major Consequences of Certain US Courses of Action on Cuba. SNIE 11-19-62. Washington, Oct. 20, 1962.

Matveyev in IZVESTIYA. FBIS-FRB-62-211. Washington, Oct. 28, 1962.

Memorandum for the Record: Notification of NSC Officials of Intelligence on Missile Bases in Cuba. Cline. Washington, Oct. 27, 1962.

Nesterov Talk to Japan. FBIS-FRB-62-210. Washington, Oct. 26, 1962.

Notes on October 21, 1962 Meeting with the President. Robert S. McNamara, Washington, Oct. 21, 1962.

On 25 October Meeting. FBIS-FRB-62-210. Washington, Oct. 26, 1962.

Party Paper Doubts U.S. Sanity on Cuba. FBIS-FRB-62-209. Washington, Oct. 25, 1962.

Pyongyang Rally Scores U.S. Cuba Action. FBIS-FRB-62-211. Washington, Oct. 29, 1962.

Recorded Excerpts. FBIS-FRB-62-210. Washington, Oct. 26, 1962.

Report to the President's Foreign Intelligence Advisory Board on Intelligence Community Activities Relating to the Cuban Arms Build-Up. Report of the Office of the Director of Central Intelligence. Washington, April 14-October 14, 1962.

Review of West German Radio and Press. FBIS-FRB-62-203. Washington, Oct. 17, 1962.

Shragin on Two-Way Missile Withdrawal. FBIS-FRB-62-211. Washington, Oct. 29, 1962.

Shragin on U.S. 'Big Lie'. FBIS-FRB-62-209. Washington, Oct. 25, 1962.

Soviet Government Statement. FBIS-FRB-62-207. Washington, Oct. 23, 1962.

Soviet Reactions to Certain US Courses of Action on Cuba. SNIE 11-18-62. Washington, Oct. 19, 1962.

Special National Intelligence Estimate: The Threat to US Security Interests in the Caribbean Area. SNIE 80-62. Washington, Jan. 17, 1962.

Summary Record of NSC Executive Committee Meeting. EXCOM No. 5. Washington, Oct. 25, 1962.

Summary Record of NSC Executive Committee Meeting. EXCOM No. 6. Washington, Oct. 26, 1962.

Summary Record of NSC Executive Committee Meeting. EXCOM No. 7. Washington, Oct. 27, 1962.

Summary Record of NSC Executive Committee Meeting. EXCOM No. 8, Washington, Oct. 27, 1962.

Summary Record of NSC Executive Committee Meeting. EXCOM No. 10. Washington, Oct. 28, 1962.

Supplement 8 to Joint Evaluation of Soviet Missile Threat in Cuba. Guided Missile and Astronautics Intelligence Committee, Joint Atomic Energy Intelligence Committee, National Photographic Interpretation Center. Washington, Oct. 28, 1962.

Talk on Cuban Slogan. FBIS-FRB-62-204. Washington, Oct. 18, 1962.

The Crisis: USSR/Cuba. CIA Memorandum, Washington. Oct. 24, 1962.

The Crisis: USSR/Cuba Information as of 0600. CIA Memorandum. Washington, Oct. 27, 1962.

Underground Tests: Cuba Topics in Geneva. FBIS-FRB-62-208. Washington, Oct. 24, 1962.

U.N. Emergency Session Discusses Cuba. FBIS-FRB-62-209. Washington, Oct. 25, 1962.

U.S. Announces Mobilization Procedure. FBIS-FRB-62-206. Washington, Oct. 22, 1962.

U.S. Gallup Poll on Cuba. FBIS-FRB-62-205. Washington, Oct. 19, 1962.

U.S. Khrushchev Message Impact. FBIS-FRB-62-210. Washington, Oct. 26, 1962.

USSR Church Heads' Appeals. FBIS-FRB-62-10. Washington, Oct. 26, 1962.

USSR Offer to U.S. on Cuba Reported. FBIS-FRB-62-203. Washington, Oct. 16, 1962.

Wanguemert Comments on Several Topics. FBIS-FRB-62-203. Washington, Oct. 17, 1962.

Washington Report. FBIS-FRB-62-210. Washington, Oct. 26 1962.

Journal Articles

Arena, Maria do Céu Pinto. "Changing Foreign Policy: the Obama Administration's Decision to Oust Mubarak." *Revista Brasileira de Política Internacional* 60, no. 1 (2017).

Barron, Owen. "A Missed Chance? Obama on Democracy in Egypt." *Harvard International Review* 31, no. 2 (2009): 12-13.

Bundy, McGeorge, and James G. Blight. "Transcripts of the Meetings of ExComm." *International Security* 12, no. 3 (Winter 1987-1988).

Cyr, Arthur. "How Important is National Security Structure to National Security Policy?" *World Affairs* 146, no. 2 (1983): 127-147.

Davies, John Paton Jr. "China Hand: An Autobiography." *Foreign Affairs* 91, no. 3 (2012): 191-92.

Dorman, David. "Open Source Software and the Intellectual Commons." *American Libraries* 33, no. 11 (2002): 51-54.

Eldridge, Christopher, Christopher Hobbs, Matthew Moran. "Fusing Algorithms and Analysts: Open-Source Intelligence in the Age of 'Big Data.'" *Intelligence and National Security* 33, no. 3: 391-406.

George, Alexander L. "The case for multiple advocacy in making foreign policy", *American Political Science Review* 66, no. 3 (1972): 751-85.

Gibson, Stevyn D. Gibson. "In the Eye of the Perfect Storm: Re-imagining, Reforming and Refocusing Intelligence for Risk, Globalisation and Changing Societal Expectation." *Risk Management: An International Journal* 7, no. 4 (2005): 23-41.

Glassman, Michael, and Min Ju Kang. "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)." *Computers in Human Behavior* 28, no. 2 (2012): 673-682.

Haynes, Darren R., and Francesco Cappa. "Open-Source Intelligence for Risk Assessment." *Business Horizons* 61, no. 5 (2018): 689-697.

Hilsman, Roger Jr. "Intelligence and Policy Making in Foreign Affairs." *World Politics* 5, no. 1 (1952): 1-45.

Holt, Karen M. "Strengthening Presidential Decision-Making Capacity". *Presidential Studies Quarterly* 30, no. 1 (2000): 27-46.

Richard H. Immerman, "Intelligence and Strategy: Historicizing Psychology, Policy, and Politics," *Diplomatic History* 32, No. 1 (2008), 1-23.

Kolodziej, Edward A. "The National Security Council: Innovations and Implications." *Public Administration Review* 29, no. 6 (1969): 573-585.

Lindblom, Charles E. "The Science of 'muddling' through.'" *Public Administration*. *Review* 19, Spring (1959): 79-88.

MacDonald, Margaret S., and Anthony G. Oettinger. "Information Overload: Managing Intelligence Technologies." *Harvard International Review* 24, no. 3 (2002): 44-48.

Madill, Donald L. "Producing Intelligence from Open Sources." *Military Intelligence Professional Bulletin* 34, no. 4 (2005): 19-25.

Mady, Abdel-Fattah. "Popular Discontent, Revolution, and Democratization in Egypt in a Globalizing World." *Indiana Journal of Global Legal Studies* 20, no. 1 (2013): 313-337.

Mercado, Stephen. "Sailing the Sea of OSINT in the Information Age: A Venerable Source in a New Era," *Central Intelligence Agency Library* 48, no. 3 (2004).

Merey, Daniel S., et al. "Leader, Follower, or Spectator? The Role of President Obama in the Arab Spring Uprisings." *Social Science Quarterly* 93, no. 5 (2012): 1185-1201.

Moshirnia, Andrew V. "Valuing Speech and Open Source Intelligence in the Face of Judicial Deference." *Harvard National Security Journal* 4, no. 2 (2013): 385-454.

Newmann, William W. "The Structures of National Security Decision Making: Leadership, Institutions, and Politics in the Carter, Reagan, and G.H.W. Years." *Presidential Studies Quarterly* 34, no. 2 (2004): 272-306.

Pascovich, Eyal. "Intelligence Assessment Regarding Social Developments: The Israeli

Experience." *International Journal of Intelligence and Counterintelligence* 26, no. 1 (2013): 84-114.

Pfiffner, James P. "Presidential Decision Making: Rationality, Advisory Systems, and Personality." *Presidential Studies Quarterly* 35, no. 2 (2005): 217-218.

Pillar, Paul R. "Intelligence, Policy, and the War in Iraq." *Foreign Affairs* 85, no. 2 (2006): 15-27.

Rashed, Mohammed Abouelleil, and Islam El Azzazi. "The Egyptian Revolution: A Participant's Account from Tahrir Square January and February 2011." *Anthropology Today* 27, no. 2 (2011): 22-27.

Ray, Aswini K. "Political Economy of the National Security Council." *Economic and Political Weekly* 25, no. 9 (1990): 424-426.

Reynolds, P.A. "Non-State Actors and International Outcomes." *British Journal of International Studies* 5, no. 2 (1979): 91-111.

Rosati, Jerel A. "Jimmy Carter, a Man Before His Time? The Emergence and Collapse of the First Post-Cold War Presidency." *Presidential Studies Quarterly* 23, no. 3 (1993): 459-476.

Setzekorn, Eric. "Open Source Information and the Office of Naval Intelligence in Japan." *International Journal of Intelligence and Counterintelligence* 27, no. 2 (2014): 368-386.

Sokolaw, Shalom. "Publish and Perish? The Cuban Missile Crisis and Journalists' Right to Inform Versus Their Responsibility to Withhold." *New York History* 85, no. 3 (2004): 265-275.

Smith, Dale L. "Reagan's National Security Legacy: Model Based Analyses of Recent

Changes in American Policy". *The Journal of Conflict Resolution* 32, no. 4 (1988): 595-625.

Tufekci, Zeynep. "Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square." *Journal of Communication* 62, no. 2 (2012): 363-379.

Legislation

Combatant Commands, U.S. Code 6 (2011) §161-168.

Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433, *U.S. Statutes at Large* 100 (1985): 992.

Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108-458, *U.S. Statues at Large* 118 (2004): 3638.

National Security Act of 1947. Public Law 80-253, *U.S. Statues at Large* 61 (1947): 495.

Other Periodicals and Websites

Agrawal, Nina. "There's more than the CIA and FBI: the 17 agencies that make up the U.S. Intelligence Community." *Los Angeles Times* (Los Angeles, CA), Jan. 17, 2017.

Coleman, David. "NSC ExComm Meetings, 1962-1963". History in Pieces. https://historyinpieces.com/research/meetings-excomm-executive-committee-national-security-council (accessed March 1, 2019).

"Combatant Commands." United States Department of Defense. https://www.defense.gov/Know-Your-Military/Combatant-Commands/ (accessed

December 29, 2018).

Broad, Ellen. “Are Cambridge Analytica’s insights even that insightful?”. *The Guardian* (London, UK), March 22, 2018.

Dubberley, Sam. “How open source evidence took a lead role in the response to the Douma chemical weapons attack.” *Amnesty International* (Boston, MA), April 23, 2018.

Draeger, Walter R. “Take advantage of OSINT.” *U.S. Army Intelligence Center and School* (Sierra Vista, AZ), July 1, 2009.

Fitfield, Anna. “With technology, these researchers are figuring out North Korea’s nuclear secrets.” *The Washington Post* (Washington, DC), Nov. 21, 2017.

Hern, Alex. “Google says machine learning is the future. So I tried it myself”. *The Guardian* (London, UK), June 28, 2016.

“INTelligence: Open Source Intelligence,” *Central Intelligence Agency: Featured Story Archive*, (Washington, D.C.), August 6, 2018.

Jay, Alexander. “The role of social media in the 2011 Egyptian revolution.” *Student Voices* (New York, NY), June 1, 2016.

Johnson, Loch K. “The Aspin Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission.” *Central Intelligence Agency Library* (Washington, D.C.), April 14, 2007.

“Kisstadion.” Hungarian Ministry of Human Resources. https://www.kulturinfo.hu (accessed April 19, 2019).

Lapowsky, Issie. “The man who saw the dangers of Cambridge Analytica.” *Wired* (London, UK), June 19, 2018.

May, Ernest R. "John F. Kennedy and the Cuban Missile Crisis." *BBC History* (London, UK), November 18, 2013.

"Part Three: Military Intelligence Disciplines." *Global Security*. https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap5.htm (accessed January 30, 2019).

Schwirtz, Michael, Ellen Barry. "Armchair Investigators at Front of British Inquiry Into Spy Poisoning." *The New York Times* (New York, NY), October 9, 2018.

Shearlaw, Maeve. "Egypt five years on: was it ever a 'social media revolution'? : Tahrir Square's spirit of change was infectious, but activists looking back say Facebook and Twitter were just tools, never the driving force." *The Guardian* (London, UK), Jan. 25, 2016.

Thiessen, Marc. "Obama blew it in Egypt—again." *The Washington Post* (Washington, DC), July 8, 2013.

"Timeline of the Cuban Missile Crisis." Atomic Archive. http://www.atomicarchive.com/History/cuba/timeline.shtml (accessed: February 10, 2019.

Tufekci, Zeynep. "How Social Media took us from Tahrir Square to Donald Trump." *MIT Technology Review* (Cambridge, MA), August 14, 2018.

Vargas, Jose Antonio. "Spring Awakening: How an Egyptian Revolution Began on Facebook." *The New York Times* (New York, NY), Feb. 17, 2017.

Feaver, Peter. "What is grand strategy and why do we need it?", *Foreign Policy* (Washington, D.C.), April 8, 2009.

Reports

Best, Richard A., Jr., and Alfred Cumming. *CRS Report for Congress: Open Source Intelligence (OSINT) Issues for Congress*. Washington: Congressional Research Service (Library of Congress) Report, 2007.

Department of State National Interests and Strategic Goals. Washington: Office of Website Management, Bureau of Public Affairs (United States Department of State), 2010.

Foreign Broadcast Information Service History Part III: 1957-1967. Washington: The Directorate of Intelligence Historical Series, 1972.

History of the National Security Council: 1947-1997. Washington: Office of the Historian, 1997.

Open-Source Intelligence. Headquarters of the Department of the Army. Washington: 2012.

Intelligence Community Civilian Joint Duty Program. Washington: Office of the Director of National Intelligence, 2013.

Intelligence Community Joint Duty DoD Swap Pilot: Many Perspectives One Community. Washington, Defense Civilian Intelligence Personnel System, 2006.

Kean, Thomas H., et al. The 9/11 Commission Report. Washington: The 9/11 Commission Members & Staff, 2004, 413.

Kobb, Larry, and Michael Kraig. Winning the Peace in the 21st Century. Muscatine: Task Force Report, 2003.

Moens, Alexander A. The Multiple Advocacy Strategy and the Role of the Custodian: the Carter Years. Vancouver: Faculty of Graduate Studies (Department of Political

Science) at the University of British Columbia, 1988.

"National Security Council." Washington: Executive Office of the President of the United States, 2019.

Offenhauer, Priscilla. General and Flag Officer Authorizations for the Active and Reserve Components: A Comparative and Historical Analysis. Washington: Federal Research Division of the Library of Congress Report, 2007.

Silberman, Laurence H., et al. Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Washington: Members & Staff of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005.

The National Security Strategy of the United States of America. Washington: The White House 2002, Preface.

Williams, Heather J., and Illana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Boston: The RAND Corporation, 2018.

Zegart, Amy. The Cuban Missile Crisis as Intelligence Failure. Stanford: Hoover Institution Policy Review, 2012.