CROSSING THE RUBICON:
INVESTIGATING CONGRESSIONAL OVERSIGHT OF THE INTELLIGENCE COMMUNITY

by
Ralph W. Corey

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Government

Baltimore, Maryland
May 2014

Abstract – There is a common narrative among researchers and experts that congressional bipartisanship among intelligence overseers is decreasing and effectiveness is increasingly degraded. The Senate Select Committee on Intelligence has historically demonstrated strong bipartisanship as a result of its organization and leaders. Changing trends among committee membership and voting since the committee's inception suggests the environment is shifting. There is evidence of modest increases in partisan membership and increasingly divided "yea" votes by committee members on significant national security legislation. However, examining open hearing dialogue suggests its necessary to maintain a more nuanced perspective of oversight partisanship and effectiveness. In the cyber domain, the Senate Select Committee on Intelligence demonstrates strong public advocacy and actively addresses constitutional adherence by the Intelligence Community. The committee does not however, effectively provide the Intelligence Community important strategic guidance. Despite shortfalls, public perceptions of intelligence oversight are generally positive. Public opinion among informed respondent's supports "hands-on" intelligence oversight with an understanding of the secrecy required by intelligence overseers. Respondents recognize the negative effects of partisanship and reinforce the significance of existing oversight institutions. There is support for some changes in intelligence oversight to improve effectiveness, but no indication respondents believe the system is in need of major change. *Crossing the Rubicon* explores each of these important intelligence oversight issues with objective and methodical analysis. The research provides academics and legislators unique data regarding a critical government function. Intelligence oversight has a responsibility to

ensure American ideals are protected and the Intelligence Community operates effectively within prescribed boundaries.

Thesis Advisors - Dr. Jennifer Bachner, Dr. Kathryn Wagner-Hill, Dr. Dorothea Wolfson

Acknowledgements – I would like to thank my wife, daughter, and parents for their love and support. I would also like to thank Professor Jennifer Bachner, Professor Kathryn Wagner Hill, and Professor Dorothea Wolfson for their guidance, advice, and expertise.

Table of Contents

List of Tables

List of Figures

THE FOUNDATION FOR EXPLORATION

Examining the Intelligence Community (IC) is like passing the point of no return. The IC is a decentralized labyrinth of institutions indispensible to the U.S. national security apparatus. The nature of studying the IC and its associated oversight institutions is inhibited by secrecy, but essential given the relationship between the IC and American citizens. Researchers who study the IC and intelligence oversight must simultaneously understand the complex dynamics of congressional politics and the unique structure of the U.S. IC. After "crossing the Rubicon" to study intelligence oversight it is impossible to follow a direct path to a conclusion. Instead there are dead ends, course corrections, and reversals that reveal the complexity of the situation and illuminate the lack of clear solutions to improving intelligence oversight. Despite shortfalls, Americans can rest assured intelligence oversight by Congress is vigorously conducted each day with a central focus towards national security and American civil liberties.

The Senate Select Committee on Intelligence (SSCI) has unique oversight responsibilities for the IC and an important role in balancing preservation of personal freedoms with protection of national security. Effective oversight of the IC is critical to providing clear boundaries and limits for executive action. Effective oversight of the IC also has an important role in providing informed national strategic policy recommendations. The secrecy surrounding the IC limits the ability of third parties to serve as additional sources of oversight. Therefore, in an interconnected world where a seemingly innocuous intelligence operation has the potential to cause global repercussions, the SSCI serves as an important counter-balance to the executive branch. *Crossing the Rubicon: Investigating Congressional Oversight of the Intelligence*

Community is an in-depth study into congressional oversight of the IC with a focus on the SSCI.

Modern democratic thought is imbued with the idea that citizens authorize elected representatives to take action on their behalf, while representatives are simultaneously held accountable for those actions through elections. Schmitter and Karl provide a useful definition for the theoretical foundation in researching congressional oversight of the IC and the effectiveness of the SSCI. They offer that "[m]odern political democracy is a system of governance in which rulers are held accountable for their actions in the public realm by citizens, acting indirectly through the competition and cooperation of their elected representatives."[1] The U.S. system of governance is outlined in the U.S. Constitution. It gives the government its structure and it provides the government boundaries in its relationship with American citizens. It dictates that the U.S. will be a state ruled by laws. Those concepts frame the options the government has at its disposal for conducting intelligence in defense of the state. If dissatisfied with intelligence policy within the executive branch or intelligence oversight within the legislative branch the citizenry has elections at its disposal in order to change representation. Schmitter and Karl also identify the public realm where the government is authorized to act in traditional American liberal thought, is often narrowly defined to protect freedom. These concepts are directly connected to American perceptions of a secretive IC and the trust Americans have in their government.

[1]Phillipe C Schmitter and Terry Lynn Karl, "What democracy is...and is not," In *Essential Readings In Comparative Politics.*, eds. Patrick H. O'Neil, Ronald Rogowski. 4th ed., (New York: WW Norton & Company Inc, 2006), 204. Schmitter and Lynn Karl derive their definition of democracy from Joseph Schumpeter who defined democracy as an "institutional arrangement for arriving at political decisions in which individuals acquire the power to decide by means of competitive struggle for the people's vote" (pg. 212). However, Schmitter and Lynn Karl note that Schumpeter's definition for democracy failed to address the role of accountability and other methods of competition beyond the vote that existed.

There is more to congressional oversight than the idea that unresponsive legislators fail to win reelection. Robert Dahl suggests that in any democracy there is a "democratic bargain" that exists between the government and the citizenry, whereby the citizenry agree to obey the laws enacted by their representatives even if the opposition was voted into power.[2] There is a trust in the elected government and in the system to allow for predetermined future elections. Democracy only works if both sides trust that everyone will abide by the rules laid out in constitution. These foundational principles allow the U.S. government to enact legislation that builds an IC designed to spy on U.S. adversaries. They also begin to dig at the theoretical reasons intelligence oversight exists.

According to the U.S. Constitution, Congress shall have the power to "make all laws which shall be necessary and proper for carrying into execution the foregoing powers, and all other powers vested by this constitution in the government of the United States, or in any department or officer thereof."[3] Herein lies the foundation for oversight, Congress is enabled to ensure that the executive branch carries laws into execution as prescribed in Article I, Section 8. Joel Aberbach adds substance to Congress' responsibility by suggesting that oversight helps prevent executive branch abuses of power and holds the president accountable for his actions. He defines oversight as "congressional review of the actions of federal departments, agencies, and commissions and of the programs and policies they administer."[4] The 1946 Legislative Reorganization

[2] Ibid., 208.
[3] The U.S. National Archives & Records Administration, *The Constitution of the United States: A Transcription*., (September 17, 1787).
[4] Joel D Aberbach, "Changes in congressional oversight," *The American Behavioral Scientist* 22 no.5 (1979): 494-495.

Act created "continuous watchfulness" by the legislature over the executive branch.[5] In 1976, the SSCI was created to service oversight of the IC for Congress and U.S. citizens.

Each chapter in *Crossing the Rubicon* explores a different facet of IC oversight. Considerable scholarship is devoted to studying the SSCI and this research builds upon the past and adds rebuttals and nuance to the narrative of dysfunctional or irrelevant oversight. Chapter one explores growing trends in partisan membership on the SSCI and evaluates roll call data on national security related legislation over the last thirty years. Chapter two has a more narrow scope and studies the SSCI's oversight of the IC in the cyber domain from 2003 to 2013. In a case study of open hearings the SSCI is evaluated on four principles of oversight effectiveness. In chapter three an informed public reveals its perceptions of intelligence oversight through a public opinion survey that uniquely advances scholarship on IC oversight.

Chapter One. "Voting for National Security," studied changes in partisanship among SSCI members and associated voting trends on national security related legislation. Membership data, dynamic-weighted nominate scores, and senate roll call data, alongside other control variables served as the foundation to a panel data set, from which conclusions could be drawn on changes in the SSCI over time. The data revealed modest increases in the strength of partisan leanings among SSCI membership over the course of its history. In addition, voting trends became slightly more polarized over time. The results supported other scholarship that suggested the SSCI had lost some of its bipartisan heritage. It highlighted a disconcerting trend towards increased partisan membership that could inhibit the SSCI's ability to gather consensus for action.

[5] Ibid., 493.

There is a line of thought arguing increased partisan membership on the SSCI is useful for energizing investigations and reviews. In preventing IC violations of law it is important to have members paying close attention to policies and programs implemented by the executive branch, even if the motivation to do so stems from a place of political opposition. However, there is a thin line of effective oversight between politically driven oversight that degrades the trust between the IC and legislative overseers versus energized oversight motivated by a desire to improve national security, defend civil liberties and capitalize on political missteps of an oppositional administration. Chapter two tackled the thin line of effective oversight.

Chapter Two. "The Cyber Domain: A Case Study in Oversight Effectiveness," was a targeted review of SSCI oversight in the cyber realm. Reviewing open hearings over the course of ten years illuminated the challenge to overcoming the topic du jour and providing effective oversight in a single policy area. The SSCI was evaluated during open hearing dialogue on its ability to offer the IC strategic guidance, ensure IC constitutional adherence, demonstrate legislative activism, and provide public advocacy. This qualitative assessment of SSCI oversight effectiveness in the cyber realm identified strong public advocacy in a bipartisan manner during open hearings. However, it also demonstrated the difficulty for policymakers to provide "over the horizon" oversight to the IC.

"The Cyber Domain: A Case Study in Oversight Effectiveness," suggests legislators are paying attention to oversight issues as they arise and IC issues are not ignored. It also suggests the rhetoric between SSCI members in open hearings is productive and fosters a bipartisan atmosphere. The challenges to effective oversight

revealed in chapter two revolve around strategic guidance to the IC. Committee members in conjunction with the IC, the executive branch, and the private sector need to clarify the operating environment's boundaries. Partisanship plays a small role in philosophically different approaches to IC freedom in the cyber domain, but overseers are most challenged by the complexity of the problem. More importantly, the complexity of the cyber operating environment, changing technology, and a lack of effective legislation leave SSCI members ill-equipped to provide very effective oversight.

Chapter Three. "If Angels Were to Govern Men," examined the public's opinion of intelligence oversight. The IC is dependent upon public perceptions of legitimacy to ensure congressional support and funding. National security issues require some level of transparency to American citizens. Through an online public opinion survey it was possible to identify perceptions of IC oversight and assess areas legislators could improve perceptions. Survey questions were designed to evaluate the significance of IC oversight to the public, perceptions of oversight effectiveness, and the structure of congressional oversight. The survey helps to better organize IC oversight issues based on respondent opinions.

The results suggested respondent's believed the oversight committees were important institutions and somewhat effective. This conclusion was buttressed by perceptions the committees were in need of some structural changes to provide more effective oversight. A strong majority of respondents supported a "hands-on" approach to intelligence oversight with a broad diversity of opinions regarding the primary purpose of oversight. Respondents leaned towards allowing intelligence oversight more secrecy than transparency, while a plurality believed oversight failures were most often the result

of failing to understand a problem. Although, the results were not representative of all American citizens, they provided a useful data set from informed observers of intelligence oversight. Chapter three offers a completely unique assessment of congressional oversight of the IC.

In the context of the American democratic experiment, the institution of congressional IC oversight is in need of some changes, but remains relevant to the U.S. democratic system of governance and is considered important by American citizens. *Crossing the Rubicon* is a rebuttal to arguments that the SSCI should be dismantled. It is a confirmation of the perceived and actual added value of congressional oversight. It criticizes various aspects of congressional oversight provided by the SSCI, specifically the direction it provides the IC and the influence of partisanship. Some shortfalls in congressional oversight are externally influenced, such as the committee's limitation in appropriating power. However, this research highlights shortfalls to oversight internal to the SSCI, which means committee members can make changes. All three chapters evaluate different issues related to congressional oversight of the IC. However, without historical perspective of the formal oversight institutions in place today, it is impossible to understand the role and importance of intelligence oversight.

HISTORY AND INTENT

Before the mid-seventies, oversight of the IC was largely an informal process. Following the end of the Cold War, oversight was vested in the Senate Armed Services Committee and dominated by its Chairman, Senator Richard Russell (D- Georgia). Russell viewed the newly created Central Intelligence Agency (CIA) in a positive light and for years

ensured any attempts of others to claim oversight responsibility of the IC was rebuffed.[6] In time however, the Watergate scandal, the conflict in Vietnam and the overthrow of the democratically elected government in Chile contributed to the demand for congressional action. As the Cold War consensus dissolved the *New York Times* article by Seymour Hersh in December 1974 laid bare a multitude of CIA indiscretions and became the catalyst for a congressional response. The Church Committee was established following revelations of CIA domestic spying and FBI operations targeting civil rights activists and anti-war protests.[7] Ultimately, the Church Committee found misconduct on the part of the IC significant enough to warrant the establishment of a permanent congressional oversight body.[8][9] Watergate, Vietnam, and conclusions of the Church Committee all contributed to growing distrust in the government. The mood of the mid-seventies demanded increased oversight, but by creating the SSCI, Congress was forced to grapple with the conflict between personal liberty and national security as it related to the secretive IC.[10][11]

The SSCI was endowed with a number of significant responsibilities and left pining for others. They were authorized to legislate on all matters relating to the IC, investigate allegations of misconduct and to monitor and audit programs. The Senate was given the responsibility to confirm senior IC officials, and the SSCI was to be provided

---

[6] Marvin C. Ott, "Partisanship and the Decline of Intelligence Oversight," *International Journal of Intelligence and Counterintelligence* 16 no.1 (2003): 74.
[7] For an extensive review of the Church Committee --it's formation, members, mission, and politics-- read Loch Johnson's *A Season of Inquiry* for first hand accounts and insights.
[8] James S. Van Wagenen, "A Review of Congressional Oversight," *Studies in Intelligence* 40 no.5 (1997): 99.
[9] Ott, "Partisanship and the Decline of Intelligence Oversight," 74.
[10] Stephen F. Knott, "The Great Republican Transformation on Oversight," *International Journal of Intelligence and Counterintelligence* 13 no.1 (2000): 51.
[11] Loch Johnson, "Ostriches, Cheerleaders, Skeptics, and Guardians: Role Selection by [US] Congressional Intelligence Overseers," *SAIS Review of International Affairs* 28 no.1 (2008): 96.

prior notification of covert actions and given access to sensitive IC information.[12] However, the committee also competed with existing oversight institutions in two important regards. First, it was only created with jurisdiction for authorizing the National Foreign Intelligence Program (NFIP) --meaning they authorized the CIA's budget-- but no power to appropriate funds to IC programs.[13] This left a constant tension between "hollow budget authorities" provided to the SSCI and "appropriated but not authorized" budget control in the Appropriations Committee.[14][15] Second, for intelligence matters of a defense nature, the Senate Armed Services Committee contained oversight responsibilities for many Department of Defense entities and left the SSCI with an institutional weakness regarding control over a significant portion the IC.[16] Considering the two weaknesses, the only silver lining for the SSCI was the motivation for stronger internal relationships and better relationships with IC officials, which over time improved the committee's credibility and stature.

The need for an intelligence apparatus is wrapped up in the prevention of strategic surprise and the ability to gain a strategic advantage for policymakers. However, intelligence oversight exists to maintain the public's trust and the legitimacy of governmental institutions. In analyzing the intelligence communities of new democracies

---

[12] Ott, "Partisanship and the Decline of Intelligence Oversight," 77-78.
[13] Gregory C. McCarthy, "GOP Oversight of Intelligence in the Clinton Era," *International Journal of Intelligence and CounterIntelligence* 15 no.1 (2002): 29.
[14] Mark M. Lowenthal. *Intelligence: From Secrets to Policy*. 4th ed. (Washington DC: CQ Press, 2009), 205-206.
[15] In a 13 November 2007 statement before the SSCI former Vice Chairman of the 9/11 Commission Mr. Lee Hamilton commented on intelligence oversight, highlighting that the Defense Appropriations Sub-Committee on Intelligence gets overburden, in turn hindering effective IC oversight. However, the IC knows where appropriations take place and could seek Appropriations Committee support as an end around to the SSCI if desiring money for an unauthorized program.
[16] The Department of Defense makes up a significant portion of the 16 member intelligence community; to include the Defense Intelligence Agency, the National Security Agency, the National Geo-Spatial Intelligence Agency, National Reconnaissance Organization, intelligence departments at each of the combatant commands and individual units within the military services.

Florina Matei and Thomas Bruneau point out that although effectiveness is often dependent on secrecy, trust is built upon transparency.[17] The same concept applies in the U.S. and effective oversight is a piece of the transparency puzzle required to ensure public support for IC budgets and programs. The Iran-Contra scandal exemplifies the debate between secrecy and openness.[18] David Colton argues the congressional oversight debate following the Iran-Contra Scandal was misguided and skewed the separation of powers designed into American democracy. Colton disagrees with a statutory approach to oversight and suggests, "[a]ny oversight mechanism needs to be broad and flexible enough to encompass the entirety of the intelligence community and the realities of the fragmented power within it."[19] The decentralized nature of today's IC reinforces his comment and calls into question the structure of congressional oversight institutions.[20] There is widely accepted scholarship that fragmented authorities within the SSCI and HPSCI add significant obstacles to effective oversight. Couple poor oversight structure with limited information on committee activities, and the public is challenged to participate in the political process.

Each chapter in *Crossing the Rubicon* tackles the challenging task of assessing the oversight institutions Congress has created to triangulate enhanced national security, protecting American civil liberties, and effectively overseeing the IC. The term

---

[17] Florina Christiana Matei and Thomas Bruneau, "Policymakers and Intelligence Reform in New Democracies," *International Journal of Intelligence and Counterintelligence* 24 (2011): 663-665.
[18] Iran-Contra was a covert CIA operation in which the Contra rebels in Nicaragua were provided funds to fight the government as a result of the secret sale of weapons to Iran in an effort to secure the release of American hostages.
[19] David Everett Colton, "Speaking Truth to Power: Intelligence Oversight in an Imperfect World," *University of Pennsylvania Law Review* 137 no.2 (1988): 575-579.
[20] Following the terrorist attacks against the U.S. on September 11, 2001, President Bush was granted broad authorities to execute the "Global War on Terrorism," through passage of the USA PATRIOT Act. However, this statutory authority still reflects the legalistic approach to oversight rejected by Colton as he might suggest the President derives the authority to initiate intelligence programs without congressional authorization in his execution of foreign affairs. Several actions taken by President Bush were argued to fall under Article II authority.

"oversight" is interesting because it can be defined as "watchfulness" or a "failure to notice something."[21] The SSCI is tasked to provide the former and avoid the latter, while this thesis seeks to explain how well it performs this important governmental function. Most broadly, the literature tends to glorify the first fifteen years of the committee and suggests a less than stellar record in the last twenty years. Chapter One: "Voting for National Security," generally supports that narrative while Chapter Two: "The Cyber Domain," calls for pause and consideration that the SSCI is in tune with IC actions or responds only when called upon. Chapter Three: "If Angels Were to Govern Men," adds the element of public opinion to an assessment of oversight effectiveness. IC oversight receives more favorability than many recent polls concerning Congress and respondents suggest fewer changes are needed then the average person would assume. However, an aggregate review of SSCI members and their votes is the best starting point for a useful assessment of IC oversight.

[21] http://www.merriam-webster.com/dictionary/oversight (accessed 26 January 2014).

CHAPTER ONE: VOTING FOR NATIONAL SECURITY

Each day the IC is asked to collect volumes of information from around the globe, analyze and assess its value, and disseminate it to policymakers and political leaders. This intelligence cycle exists to protect the United States and continues regardless of which political party controls the White House or Congress. The SSCI is responsible for oversight of the IC and ensuring its members conform to the Constitution and the laws of the United States. To avoid the politicization of intelligence for political purposes, a SSCI that is dutifully executing its mission should be less partisan then other congressional oversight institutions. National security is dependent on timely and accurate intelligence and the IC is dependent on the SSCI to provide adequate resources and effective oversight.[22] If partisan politics pervade the SSCI then a degradation of national security is an eventuality. When examining the relationship between SSCI member political party affiliation and voting trends for intelligence and national security related matters, it is expected that committee members set aside partisan differences and adopt a greater degree of bipartisanship for the good of the country's security. The SSCI was founded on principles of bipartisanship, but in a review of its history, scholars suggest that these principles have been lost and partisanship is on the rise. An original quantifiable review of the voting trends and membership changes in the SSCI lent

[22] The SSCI is not the only congressional institution responsible for IC oversight. The House Permanent Select Committee on Intelligence (HPSCI) and the both the House and Senate Appropriations Defense Subcommittees have important roles in oversight as well. Those oversight bodies are beyond the scope of this research, but could be useful comparisons to SSCI trends in more broad research of congressional oversight.

considerably more data to the debate. The unique results of this study modestly support the narrative of rising partisanship within the SSCI.

CAPABILITIES AND INTENTIONS

In the years following its 1976 creation, SSCI members worked hard to gain the trust and respect of the IC. Avoiding information leaks was the basis for operating outside of the public eye with a focus on bipartisanship. Early in its history, the SSCI had senior IC officials skeptical they could be divorced from using their access to classified material for political advantage. Committee members needed to demonstrate they could protect sensitive information and handle material with the same discretion as the IC. Consequently, bipartisanship was an essential element in designing the SSCI and it was established as a select committee where party leadership selected members vice party caucuses. Membership on the committee was divided almost evenly between the two parties and included representatives from the Appropriations Committee, Armed Services, Foreign Relations, and Judiciary Committees.[23] The goal to select moderate members to the SSCI was a means to achieve bipartisan oversight and scholarly opinion reinforces that in short order that goal was achieved.[24]

Key legislative accomplishments highlight early effective oversight throughout the 1980's. The Foreign Intelligence Surveillance Act created the requirement for a court order to conduct electronic surveillance for intelligence purposes within the U.S. The Intelligence Oversight Act of 1980 reduced the notification requirements for covert action from eight committees down to the two intelligence oversight committees. The

[23] Senate Select Committee on Intelligence, *Rule of Procedure for the Select Committee on Intelligence United States Senate 112th Congress* (Washington: U.S. Government Printing Office, 2011), 14.
[24] Jennifer Kibbe, "Congressional Oversight of [US] Intelligence: Is the Solution Part of the Problem?" *Intelligence and National Security* 25 no. 1 (2010): 38.

Intelligence Identities Protection Act of 1982 criminalized the revelation of the identity of intelligence agents. The CIA Information Act of 1984 exempted specific information from Freedom of Information Act mandates.[25] During the latter half of the 1980's SSCI Chairman, Senator David Boren (D- Oklahoma) was considered an exemplar of effective oversight and bipartisanship. He served as SSCI chairman for six years and believed in a bipartisan approach to oversight of national security issues. Boren worked across the aisle to pass legislation for increased oversight following the Iran-Contra scandal, as well as legislation emphasizing the mission of the IC following the Cold War.[26] Scholars agree the 1980's marked the high point of bipartisanship for the SSCI and resulted in generally effective oversight of the IC. The SSCI chairman and vice-chairman often worked in tandem and the nonpartisan SSCI staff of the eighties were equipped with a significant intelligence background.[[27]][[28]] Unfortunately, the unique SSCI qualities in the eighties were the same qualities that fostered a rise in partisanship in the nineties.

THE RISE OF PARTISANSHIP

There are competing theories why partisanship within the SSCI began increasing in the nineties. Rising partisanship was possibly a byproduct to the Cold War's conclusion and a removed behavioral constraint --diminished consequences for making decisions based on political desires.--[29] In a similar vein, the personal ambition of Committee members to fill an IC directional vacuum left by the Cold War's end was another possible cause for

[25] Wagenen, "A Review of Congressional Oversight," 101.
[26] L. Britt Snider, *The Agency and the Hill : CIA's Relationship with Congress, 1946-2004*. (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2008), 58 & 83.
[27] Ott, "Partisanship and the Decline of Intelligence Oversight," 80.
[28] Kibbe, "Congressional Oversight of [US] Intelligence: Is the Solution Part of the Problem?" 39.
[29] Matthew B. Walker, "Reforming Congressional Oversight of U. S. Intelligence," *International Journal of Intelligence and Counterintelligence* 19, no. 4 (2007): 706.

increased partisanship.[30] The nomination of Robert Gates as the Director of Central Intelligence (DCI) for then President George H.W. Bush in 1991 was one of the first of many partisan battles.[31] "In place of an attitude that valued cooperation across political party and institutional divisions, a new 'us vs. them' mindset became dominant."[32] When Gates' nomination was in jeopardy the Bush administration called for political unity among Republicans and indicated the President wanted Gates confirmed at any cost.[33] The first among many nineties politicized events, partisanship within the SSCI often originated at the chairman.

Both SSCI Chairman Senator Arlen Specter (R- Pennsylvania) and Senator Richard Shelby (R- Alabama) were characterized as taking an "aggressive prosecutorial nature" in oversight and heavily investigated Clinton administration actions in Bosnia.[34] The nomination of Anthony Lake as DCI in 1997 was the high-water mark of partisanship. The debate over Lake's nomination broke down along strict party lines and committee members expressed their partisan positions in open forums.[35][36] Even those who argue Senator Shelby was an effective leader of the SSCI, were forced to admit that the Republican chairman reinforced partisanship when evaluating the Lake nomination.[37] Chairman leadership of the 1990's, was a significant departure from the Boren-style tactics of handling SSCI business behind closed doors. Continuing this trend, most scholars believe partisanship within the SSCI also increased during the first decade of the 21st century.

---

[30] Knott, "The Great Republican Transformation on Oversight," 57.
[31] Kibbe, "Congressional Oversight of [US] Intelligence: Is the Solution Part of the Problem?," 39.
[32] Ott, "Partisanship and the Decline of Intelligence Oversight," 84.
[33] Ibid., 82.
[34] McCarthy, *"GOP Oversight of Intelligence in the Clinton Era,"* 33.
[35] Ibid., 34.
[36] Walker, *"Reforming Congressional Oversight of U. S. Intelligence,"* 706.
[37] McCarthy, *"GOP Oversight of Intelligence in the Clinton Era,"* 34.

Scholarly research suggests the attacks on 11 September 2001 (9/11) did not usher in renewed emphasis on bipartisan approaches to intelligence oversight. In an interview, then DCI Panetta stated:

> I do believe in the responsibility of the Congress not only to oversee our operations but to share in the responsibility of making sure that we have the resources and capability to help protect this country. The only way that's going to work is if both parties are working in the same direction. There's been a lot of poison in the well in these last few years. And I think in 40 years that I've been in and out of Washington, I've never see Washington as partisan as it is today. And I think we pay a price for that in terms of trying to deal with all the problems that face this country.[38]

Whether the issue was nominations, authorization bills, commissions or investigations, scholars agreed all were occasions for partisanship within the SSCI. Mark Lowenthal noted the rising scrutiny for political appointees in the "hold" on the nomination of John Rizzo as CIA general counsel by Senator Ron Wyden (D- Oregon).[39] In previous decades the staff was selected without preference for political affiliation, but this criterion did not survive rising partisanship. The 2004 SSCI Democratic vice chairman requested the staff begin investigations into the intelligence community's role in detainee handling. However, Chairman Roberts refused to allow the investigation and left SSCI Democrats unable to review detainee handling or to conduct minority-only staff investigations.[40]

The SSCI report on intelligence estimates leading up to the war in Iraq was characterized as a politically driven report. As Senator Pat Roberts (R., Kansas) took the SSCI helm, the Iraq War intelligence estimates investigations shifted to the search for a political scapegoat. Both parties deflected blame away from their respective presidential

---

[38] Amy Zegart, "The Domestic Politics of Irrational Intelligence Oversight," *Political Science Quarterly* 126 no. 1 (2011): 5-6.
[39] Lowenthal, *Intelligence: From Secrets to Policy*. 4th ed, 210. The Democratic opposition to Rizzo's nomination was so strong it eventually led to his withdrawal.
[40] Walker, *"Reforming Congressional Oversight of U. S. Intelligence,"* 707.

candidates over the decision to go to war. Anthony Glees described the final product as a "bipartisan partisan document" and suggested Congress shifted eventual blame to the IC.[41] "The result was a Senate report which had the peculiar quality of being shaped by very different partisan political interests affecting both the Republican majority and the Democrat minority members."[42] This anecdotal evidence highlights the committee's political division over support for the War in Iraq however; both sides were able to unite behind the idea that an intelligence failure ultimately embroiled the U.S. in conflict. The scholarly evidence of rising partisanship in the SSCI since the early nineties is bountiful and the possible implications for intelligence oversight and national security provide reasons to be concerned.[43]

PARTISANSHIP AND DEFECTIVE OVERSIGHT

Increasing partisanship affects the SSCI and degrades its ability to conduct intelligence oversight. Marvin Ott notes, continuously increasing partisanship among committee members will "inevitably engender a temptation to stonewall, evade, and deceive on the part of intelligence officials."[44] Specifically, there develops more motivation to focus on executive branch relationships because IC officials operate with the expectation that anything said before the Committee will be used as political fodder.[[45]][[46]] Some

[41] Anthony Glees & Philip H.J. Davies, "Intelligence, Iraq and the limits of legislative accountability during political crisis," *Intelligence and National Security* 21 no. 5 (2006): 867.
[42] Ibid., 867.
[43] Matthew Walker and Jennifer Kibbe describe two other events that exemplify the possible increasing 21st century SSCI partisanship. First, Senate Majority Leader Bill Frist's (R- Tennessee) decision to ask the Government Affairs Committee to lead intelligence reform efforts in the Senate despite Chairman Roberts' proposed reform agenda being previously announced. The committee responsible for oversight of the IC was deemed too partisan to effectively reform it. Second the SSCI was unable to pass an annual intelligence authorization bill between 2006 and 2009. Kibbe suggests the effect was a secession of their [the SSCI's] voice in intelligence policy. Annually authorizing IC programs, budgets and activities is a primary SSCI responsibility and their failure to pass that legislation suggested they were no longer relevant in IC oversight.
[44] Ott, *"Partisanship and the Decline of Intelligence Oversight,"* 86.
[45] Walker, *"Reforming Congressional Oversight of U. S. Intelligence,"* 708.

scholars suggest increasing partisanship within the SSCI is one symptom of a larger problem with intelligence oversight. The necessary secrecy of the IC and the lack of constituencies lobbying Congress on intelligence oversight policy mean that Congress is the primary bearer of responsibility for effective oversight. Although controversial, this argument holds weight when considering the inability of third parties to provide oversight.[47][48] According to Loch Johnson, Congress "must educate the American people on the virtues of having an intelligence capability."[49] In addition to the SSCI's responsibilities for oversight, the function of intelligence is to provide unbiased information for policy making, which becomes difficult if the customer intends to use the information for political gain.

The need for bipartisanship can be likened to the need for bipartisanship within the ethics committee. In both cases the committees are without a safety net for oversight if proven ineffective. Ott aptly suggests, "as the threats become more diversified and sophisticated, the demands on intelligence collection, analysis, and operations grow apace."[50] This idea is easily supplanted to growing demands on intelligence oversight. The evolution of threats into cyberspace serves as an example of a domain where new oversight and legislative challenges face the SSCI. With these threats in mind, there is little room for partisanship.

Before studying partisan changes in the SSCI a brief discussion is warranted regarding changes within the Senate writ large. There is abundant literature and evidence

---

[46] Snider, *The Agency and the Hill : CIA's Relationship with Congress, 1946-2004*, 90.
[47] Ott, *"Partisanship and the Decline of Intelligence Oversight,"* 73.
[48] Kibbe, *"Congressional Oversight of [US] Intelligence: Is the Solution Part of the Problem?,"* 24.
[49] Johnson, *"Ostriches, Cheerleaders, Skeptics, and Guardians: Role Selection by [US] Congressional Intelligence Overseers,"* 100.
[50] Ott, *"Partisanship and the Decline of Intelligence Oversight,"* 71.

suggesting the Senate is increasing in party polarization at the same time losing incentives for bipartisanship. In the latter half of the twentieth century changes in the party system and party organization increased electoral competitiveness. When the party system suggests to both sides an opportunity to control the Senate the party organization invests a great deal more effort to win competitive races.[51] A second order effect of the change in competitiveness becomes a reduced incentive to work across party lines. It is arguable public policy is no longer the focus of Senators, gaining control of the Senate and keeping control has become the focus.

Since 1980, a shift towards excessive political messaging has also added a disincentive for bipartisan cooperation in the Senate. Frances Lee builds upon the arguments of Joseph Schlesinger as she highlights the increasing "minority" amending activity on Senate floor legislation with the explicit purpose to kill legislation and frame the debate on specific policy issues.[52] This behavior also stems from an increase in competition for Senate control. These changes in behavior and structure are buttressed with growing ideological polarization oft captured in the regular news cycle. These changes in Senate behavior run congruent to the SSCI's recent historical narrative. The SSCI was long regarded as an institution above the political fray, whether it has lost that standing is the subject of this research.

RESEARCH AND METHODS

The SSCI is not an oversight body that should succumb to highly partisan politics, but scholarly opinion suggests otherwise. Past research has commented on the effects of the

[51] Joseph A. Schlesinger, "The New American Political Party," *The American Political Science Review* 79 no. 4 (1985): 1165-1166.
[52] Frances E. Lee, "Party Politics and the Permanent Campaign on the Senate Floor." (Paper presented at the University of Maryland American Politics Workshop, February 18, 2011).

Cold War, the significance of the SSCI chairman, the role of SSCI staff, and partisan incentives for SSCI members. Much of this research was based on qualitative inquiry, drawing descriptive inference from interviews, commissions, hearings and other studies. This research quantitatively examines possible partisan shifts within the SSCI by analyzing membership and voting patterns on intelligence and national security related legislation. Previous research into the SSCI utilized anecdotal evidence to suggest rising partisanship and studied partisanship as part of a larger problem for intelligence oversight. However, assessing the effect of increasing partisanship before devoting more time to verifying its existence puts the cart before the horse. This research offers a panel data set that includes data on SSCI members gathered from its inception in the 94th Congress through the 111th Congress. The data set includes membership data, legislative action and additional influential factors that provide quantitative evidence of increasing partisanship within the SSCI.

The data on SSCI membership presented here was gathered from multiple sources, offering a wealth of information on membership, legislation and hearings. The work by Charles Stewart and Jonathan Woon on Congressional Committee assignments from the 103rd to 112th Congresses, and the work by Dr. Garrison Nelson on congressional committees from 1947 to 1992 provided the foundational data.[53][54][55] Party affiliation and dynamic-weighted nominate scores created useful independent variables.[56]

---

[53] United States Senate Select Committee on Intelligence, "*Members, Publications, Legislation*," http://intelligence.senate.gov/index.html (accessed March 4, 2012).

[54] Charles Stewart III and Jonathan Woon, *Congressional Committee Assignments*, 103rd to 112th Congresses, 1993--2011: Senate, April 12, 2011, http://web.mit.edu/17.251/www/data_page.html#0 (accessed March 4, 2012).

[55] Garrison Nelson, *Committees in the U.S. Congress*, 1947-1992, Senate, 94th to 102nd Congresses, March 10, 2008, http://web.mit.edu/17.251/www/data_page.html#0 (accessed March 4, 2012).

[56] Royce Carroll and Jeff Lewis, et. al., *DW Nominate Scores*, 1st to 111th Congresses, Senate, 94th to 111th Congresses, February 3, 2011, http://voteview.com/dwnominate.asp (accessed March 4, 2012).

However, SSCI membership has changed over time and to study changes in partisanship the research required prescribed dependent variables.

The data set includes intelligence related legislation useful for creating multiple dependent variables. The dichotomous roll call data from SSCI members on Senate floor votes allowed for quantitative analysis of SSCI voting trends. Different legislative actions were included as dependent variables because they best represented SSCI trends on intelligence related matters. The data set also includes information on the time period of legislative action and relevant congressional or governmental records. Some variables were political in nature, such as legislative action taken during a time of divided government, in a presidential election year, the political party in control of the Senate, or the length of time on the SSCI for a particular member.

In developing a method to research possible partisanship trends within the SSCI, it was important to consider that individual senators have competing interests. In some circumstances, they feel obligated to vote along party lines, where as in other cases, they possess an ideological opposition to a piece of legislation. To account for both of these possibilities it was important to include senator-specific data related to their party identification and their dynamic-weighted (DW) nominate score.

DW nominate scores were collected to identify possible shifts in partisanship within the SSCI. As Anthony Glees and Philip Davies point out, "[l]egislative oversight bodies are inhabited by political animals, creatures with deeply held and often firmly reinforced political convictions, sympathies and loyalties."[57] DW nominate scores organized as an ordered categorical variable allowed the research to account for the

[57] Anthony Glees & Philip H.J. Davies, *"Intelligence, Iraq and the limits of legislative accountability during political crisis,"* 850.

strength of partisan leanings. In this data set, committee members' scores were divided such that members described as < -0.50 were considered strongly liberal, those > -0.50, but < 0 were considered moderately liberal, those > 0, but < 0.50 were considered moderately conservative, and finally members > 0.50 were considered strongly conservative.[58] DW nominate scores, along with party identification, offered two valuable independent variables of interest that were used to study changes in the SSCI.[59]

Party identification as a Democrat or Republican was also a valuable independent variable of interest to help measure changes in SSCI partisanship. If party cohesion takes precedence over an individual member's desire to support a SSCI decision then a dichotomous variable, such as party identification, is instructive. The Republican Party unity in support of Gates' DCI nomination is an excellent example in which party identification relates the partisan nature of the issue.[60] Throughout its history, the SSCI has relied upon relationships and trust with the IC to build stature and importance within the Senate and outside of it. Independent data points such as these allowed for research into changing partisanship within the SSCI.

INTELLIGENCE AND NATIONAL SECURITY LEGISLATION

The primary purpose of this research was to gather data useful for studying partisanship trends within the SSCI. However, it is also important to take a moment and briefly assess the validity of the data gathered. Each piece of legislation selected for inclusion in the

[58] Carroll, Royce and Jeffrey Lewis, et al., *"Measuring Bias and Uncertainty in DW-NOMINATE Ideal Point Estimates via the Parametric Bootstrap,"* Political Analysis 17 (2009): 261-275. (accessed March 15, 2012)

[59] Ibid., 262-263. Dynamic-Weighted Nominate Score stands for dynamic, weighted, nominal three-step estimation. It is used to estimate the probability of "yea" votes for legislators over time using a binary choice model and based off of work by Daniel McFadden in 1976. It was developed for analysis of the U.S. House and Senate and is based on normally distributed errors. In this paper DW-nominate scores were used to estimate the ideological leaning of SSCI members based on their past voting records.

[60] Ott, *"Partisanship and the Decline of Intelligence Oversight,"* 84.

data set held unique relationships with either U.S. national security or oversight of the intelligence community. Each vote came from a SSCI member during a Senate floor vote and from a piece of legislation that at least passed the Senate. The data set is not inclusive of every piece of intelligence related legislation since the SSCI's inception, but representative of the legislative issues the SSCI has dealt with over time. There is one important assumption made regarding many of the legislative selections. Given access to unique classified information, there is an assumption that committee members' decisions are influenced by the classified intelligence they receive. The SSCI has a significant role in the security of the nation through its oversight of the IC. Therefore, the roll call votes and legislation selected for this paper were not randomly selected, but were chosen to examine the relationship between the SSCI's national security responsibilities and changes in voting along party lines.

Foreign Intelligence Surveillance Act. Evaluating the passage of the Foreign Intelligence Surveillance Act of 1978 (FISA) was an early and significant piece of legislation useful for addressing early partisanship levels in the SSCI. FISA established a specialized court to provide warrants and standard procedures for conducting electronic surveillance within the U.S. The FISA court is made up of eleven U.S. district judges and its rulings often apply to surveillance conducted by the FBI and NSA.[61] FISA was the first legislation passed that established judicial review of intelligence actions and added a component of

[61] Recently, the Foreign Intelligence Surveillance Court has garnered considerable media attention due to the release of classified documents and reporting by The Guardian, The Washington Post, and The Wall Street Journal on surveillance programs involving U.S. technology and communication firms. Under scrutiny is the balance between civil liberties and national security in the debate over the National Security Agency's ability to possibly gather volumes of data on U.S. citizens under provisions of FISA amendments and the USA PATRIOT Act passed/renewed since 9/11.

additional congressional oversight by mandating regular reports to the SSCI.[62] A review of member votes for FISA was a useful start point in evaluating partisanship during the SSCI's early years.

Intelligence Oversight Act. The Intelligence Oversight Act (IOA) of 1980 was another significant piece of legislation from early in the SSCI's history that established a baseline for evaluating partisanship among committee members. The Senate passed this charter legislation in 1980 and thus helped establish the role of the SSCI within the Senate. It reduced the number of committees and people who were informed of impending covert intelligence operations. The act was considered a legislative success in gaining oversight over executive actions, but to date, has a mixed history of achieving its stated goal for SSCI members to remain informed of presidentially directed actions.[63] This distinctive SSCI responsibility suggests it should have received bipartisan support among members.[64] The IOA had significant national security implications in protecting sensitive information and crisis response. These considerations made it essential legislation in understanding possible changes in partisanship.

Intelligence Identities Protection Act. The 97th Congress passed the Intelligence Identities Protection Act in 1982, which criminalized revealing information related to covert U.S. intelligence operatives. The legislation supported the IC and was seen as a confidence building measure between the SSCI and the IC. It was passed in the first five years of the SSCI and laid the groundwork for the relationship between overseers and the

[62] Frank J. Smits, *Congress Oversees the United States Intelligence Community, 1947-1993*. 2nd ed, (Knoxville: The University of Tennessee Press, 1994), 126.
[63] Ibid., 122-125.
[64] Smist also notes it was the leadership of Senator Birch Bayh (D-Indiana) that helped pass both the Foreign Intelligence Surveillance Act (1978) and the Intelligence Oversight Act (1980).

IC.[65] The SSCI has broad responsibilities for oversight, but must also avoid "regulatory capture" by the IC and unduly influenced by IC leadership. This legislation represented part of the bridge between the IC and the SSCI, where the SSCI was able to provide legislative support to improve IC processes and safeguards. Adding the Intelligence Identities Protection Act to the data set diversified the type of legislation collected because of its unique impacts on the IC.

INF Treaty. During the 100th Congress the Senate ratified the Intermediate-range Nuclear Forces (INF) Treaty with the Soviet Union. The leadership of Senator Boren and the role of the SSCI were essential during the ratification process. The treaty significantly effected arms control between the two states and a classified report produced by the SSCI was instrumental in renegotiating portions of the treaty.[66] The INF Treaty underscored the importance of the SSCI in matters of national security and SSCI member votes during the ratification process demonstrated the level of partisanship SSCI members brought to the final vote tally. It was an important late 1980's legislative action during Senator Boren's era of leadership and proved helpful in assessing partisanship trends in the SSCI.

FY '90 Intel Authorization Act. In the Fiscal Year (FY) 1990 Intelligence Authorization Act the SSCI incorporated a provision for an independent Inspector General (IG) for the CIA. The bill asserted the SSCI's position as overseer of agency actions and was important reform legislation following the White House's failed coup attempt in Panama. As a result of the rift between SSCI Chairman Boren and National Security Advisor Brent Scowcroft it was also a potential petri dish for partisanship between a republican

[65] Ibid., 127-128.
[66] Ibid., 272.

President and democrats on the committee.[67] The FY '90 Intelligence Authorization Act highlighted the importance of the SSCI as an oversight body and was one of the few more partisan votes among SSCI members prior to September 11th, 2001.

US Forces-Bosnia. In 1995 the 104th Congress passed Joint Resolution 44 expressing support for President Clinton's deployment of troops to Bosnia-Herzegovina. The willingness of the President to usurp congressional responsibilities for authorizing U.S. troop deployments was controversial and served as an event that galvanized a bipartisan response. In its resolution the Senate announced its support for the General Framework Agreement to create conditions for peace in the Republic of Bosnia and Herzegovina. Simultaneously, the Senate highlighted the President's decision to deploy troops without Congressional approval and their expectations the President would explain the mission and limitations of U.S. Forces.[68] SSCI members were in a unique position during the passage of this legislation to bring intelligence expertise to bear on significant national security related legislation.

USA PATRIOT Act. Signed by President George W. Bush on 26 October 2001, less than sixty days after the attacks on the World Trade Center and Pentagon, the USA PATRIOT Act received criticism for its expansion of government technical surveillance methods. Title II of the PATRIOT Act amended the Federal Criminal Code to permit wire-tapping and interception of electronic communication for use as evidence in combating terrorism. It amended the Communications Act of 1934 to permit disclosures by cable companies of subscriber information. It granted the federal government and by extension the office of

[67] Ibid., 276-277.
[68] U.S. Senate Joint Resolution 44--104th Congress, *"A joint resolution concerning the deployment of U.S. Armed Forces in Bosnia-Herzegovina,"* GovTrack.us (1995): http://www.govtrack.us/congress/bills/104/sjres44 (accessed June 3, 2013).

the President significant liberties to combat terrorism through increased electronic surveillance on computer or telephone systems, as well as provided avenues to access financial records, and altered the rights of immigrants.[69] Although signed during a time of fear and anxiety, the PATRIOT Act served as a piece of transitional legislation into the 21st century and the "Global War on Terrorism" (GWOT). It was a controversial piece of legislation due to expanded surveillance techniques, but it helps frame the last decade of SSCI voting trends.

Intelligence Reform & Terrorism Prevention Act. In October 2004, the Senate passed the Intelligence Reform and Terrorism Prevention Act (IRTPA). Driven and modeled off the recommendations of the 9/11 Commission, the IRTPA altered IC structures and functions. It established the Office of the Director of National Intelligence (ODNI), who was directed to eliminate stove-piped information routes and improve inter-agency cooperation. ODNI's duties were to serve as the head of the intelligence community, to act as the principle advisor to the President on matters of national security and to oversee and direct the National Intelligence Program.[70] The ODNI has significant challenges in authority and suffers from cultural clashes with pre-existing IC powerhouses; however, the signing of IRTPA served as another piece of legislation to assess SSCI partisanship trends in the 21st century. The IRTPA was directly related to the IC and although the Senate Government Affairs crafted the legislation, the SSCI had equities in the process and the national security implications were significant.[71]

---

[69] U.S. House Resolution 3162--107th Congress, *"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001,"* GovTrack.us (2001): http://www.govtrack.us/congress/bills/107/hr3162 (accessed April 4, 2012).
[70] U.S. Senate Resolution 2845--108th Congress, *"Intelligence Reform and Terrorism Prevention Act of 2004,"* GovTrack.us (2004): http://www.govtrack.us/congress/bills/108/s2845 (accessed April 4, 2012).
[71] Walker, *"Reforming Congressional Oversight of U. S. Intelligence,"* 704.

2006 Military Commissions Act. After the terrorist attacks on September 11th 2001, the White House ordered that "enemy combatants" would be detained for the rest of hostilities, presumably the remainder of the GWOT. The DoD responded with its own order indicating it would try "enemy combatants" using military commissions. However, in 2006 the U.S. Supreme Court invalidated the order, ruling that it fell outside the laws Congress had passed regarding the establishment of military commissions. The 2006 Military Commissions Act was Congress' response to the Supreme Court's ruling.[72] In researching partisanship within the SSCI the legislation was significant because committee members have a unique perspective on the prosecution of the GWOT. The 2006 legislation had significant national security implications and member votes had the ability to highlight growing ideological partisanship.

Improving America's Security Act. The Improving America's Security Act of 2007 implemented other recommendations of the 9/11 Commission. It was a significant piece of national security related legislation as it enhanced cooperation between federal, state, and local agencies through improved information sharing by the Department of Homeland Security (DHS). A centerpiece of the legislation was improved communication with different sectors of American society, to include the transportation sector. It specifically referenced the importance of improved rail, motor and aviation security and identified areas where the DHS should interface with entities such as the National Transportation Safety Board and the Transportation Safety Administration.[73] The voting records for the Improving America's Security Act were important to include

[72] Douglas A Hass, "Crafting Military Commissions Post-Hamdan: The Military Commissions Act of 2006," Indiana Law Journal 82 (2007): 1101-1102. The Supreme Court ruling regarding the DoD's order for military commissions came in Hamdan v. Rumsfeld.

[73] U.S. Senate Resolution 4 --110th Congress, *"Improving America's Security Act of 2007,"* GovTrack.us (2007): http://www.govtrack.us/congress/bills/110/s4 (accessed April 18, 2012).

because it was a piece of national security related legislation in which SSCI members held expertise as to the domestic vulnerabilities the U.S. faced and the persisting shortfalls in homeland security.

Protect America Act. The Protect America Act (2007) amended FISA and stated the Director of National Intelligence (DNI) could conduct surveillance of foreigners believed to be outside of the United States whose communications routed through the U.S.[74] The act also stipulated DNI and Attorney General actions were subject to review by the Foreign Intelligence Surveillance Court, but the government no longer needed a special warrant to gather foreign intelligence information of foreigners believed to be outside the U.S. and communicating with U.S. citizens inside the country. It allowed the government to work with communications services providers in gathering foreign intelligence and caused controversy over privacy issues.[75] As the SSCI approaches the second decade of the 21st century, debates continue over privacy versus security and often divide along political lines. The Protect America Act demonstrated recent partisanship trends within the SSCI.

FISA Amendments Act. In 2008 Congress passed the FISA Amendments Act in order to reform shortcomings that led to the Bush administration's warrantless wiretapping under the Terrorist Surveillance Program (TSP). Within TSP the National Security Agency was permitted to gather intelligence on U.S. citizens who were communicating with suspected Al Qaeda terrorists overseas. The provisions installed to reform FISA permitted the U.S. Attorney General in conjunction with the DNI to authorize warrantless surveillance for

[74] Stephanie Cooper Blum, "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform," *BU Pub. Int. LJ* 18 (2008): 295-296.
[75] U.S. Senate Resolution 1927--110th Congress, *"Protect America Act of 2007,"* GovTrack.us (2007): http://www.govtrack.us/congress/bills/110/s1927 (accessed April 18, 2012).

up to one year on a foreigner believed to be outside the U.S. It restricted the intentional targeting of several specified categories of persons, but did not add any requirement that the target of the surveillance be deemed an agent of a foreign power. In establishing one of the critical foundations for FISA the Supreme Court has held that particular governmental functions, such as intelligence against foreign actors, contains unique features that grant the government the ability to operate outside traditional law enforcement jurisprudence.[76] The continuing debate between civil liberties and security again placed intelligence oversight in the spotlight, making the FISA Amendments Act another important piece of legislative action for evaluating changes in SSCI partisanship.

2009 Military Commissions Act. The Military Commissions Act of 2009 was actually Title XVIII of the National Defense Authorization Act for FY 2010. The Military Commissions Act amended the Uniformed Code of Military Justice (UCMJ) and changed the language of the UCMJ concerning enemy combatants. The phrase, "unprivileged enemy belligerent" broadened the ability of the U.S. government to try terrorism suspects in military commissions.[77] Terrorism suspects, such as Khalid Sheik Muhammad, who had no affiliation to a particular military, were the targets of the amendments. The Military Commissions Act holds significant national security consequences for the treatment and management of terrorism suspects at places like Guantanamo Bay, Cuba. However, similar to the PATRIOT Act, the controversy surrounding this piece of legislation lent itself to possible increased partisan divides and was therefore useful for a study of partisanship trends within the SSCI.

---

[76] Blum, "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform," 270-299.

[77] U.S. House Resolution 2647--111th Congress, *"National Defense Authorization Act for Fiscal Year 2010,"* GovTrack.us (2009): http://www.govtrack.us/congress/bills/111/hr2647 (accessed April 5, 2012).

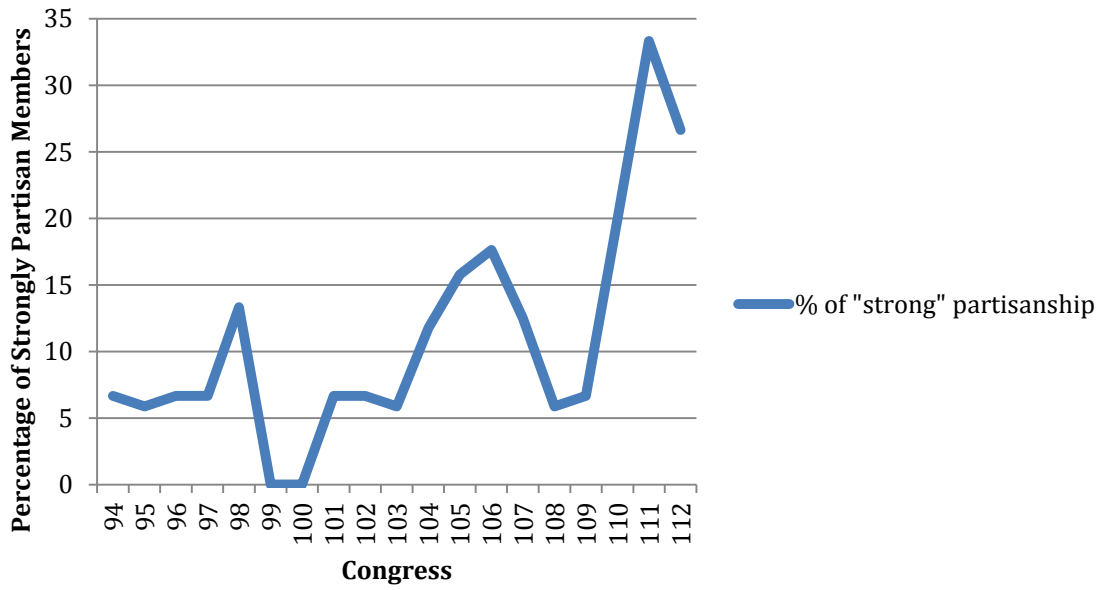
PATRIOT Sunset Extensions Act. The 2011 PATRIOT Sunset Extensions Act was unique in its unanimous Senate support. It extended three significant provisions related to terrorism prevention and electronic surveillance until June 2015. Section 206 of the USA PATRIOT Act reduced the degree of specificity for subjects of electronic surveillance under FISA. Section 206 allowed the government to seek the assistance of third parties in electronic surveillance. Critics of this provision argue there was increased potential innocent conversations could be collected using "roving" wiretaps. Section 215 of the USA PATRIOT Act was also extended until 2015. According to Edward Liu, it expanded the materials government officials could seek from private entities while simultaneously lowering the legal threshold to receive court approval for an order.[78] Critics of this provision worried about collusion between the U.S. government and the private sector. Section 6001(a) of IRTPA was the last provision extended in the Sunset Extensions Act. The "lone wolf" provision of IRTPA led to concerns about usurpation of well-established criminal law because it simplified the "evidentiary standard" for surveillance and eliminated the requirement for a suspect's connection to a foreign power.[79] All three of these provisions were designed to prevent terrorist attacks and reduced limitations for electronic surveillance by the government. However, they also served as lightening rods for contested debates over the balance between national security and civil liberties. In this respect, the Sunset Extensions Act was another important piece of intelligence related legislation where the debate easily broke along ideological lines. However, in this instance neither SSCI nor Senate votes broke along party lines in the same fashion as the debate.

[78] Edward C Liu, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, (Congressional Research Service, Library of Congress, 2012), 2-9.
[79] Ibid., 2-6.

GROWING PARTISANSHIP AMONG MEMBERS & VOTES

Analyzing the data on SSCI membership trends and voting patterns yielded unique and significant insights into partisanship levels. The data suggested a modest rise in partisanship among SSCI members since its inception. Figure 1 highlights the change in SSCI membership between 1976 and 2010 based upon the percentage of strongly liberal or strongly conservative members. The rise in members possessing strongly partisan nominate scores began in the 103rd Congress and peaked in the 111th Congress. Thirty-three percent of SSCI members in the 111th Congress held nominate scores, which fell

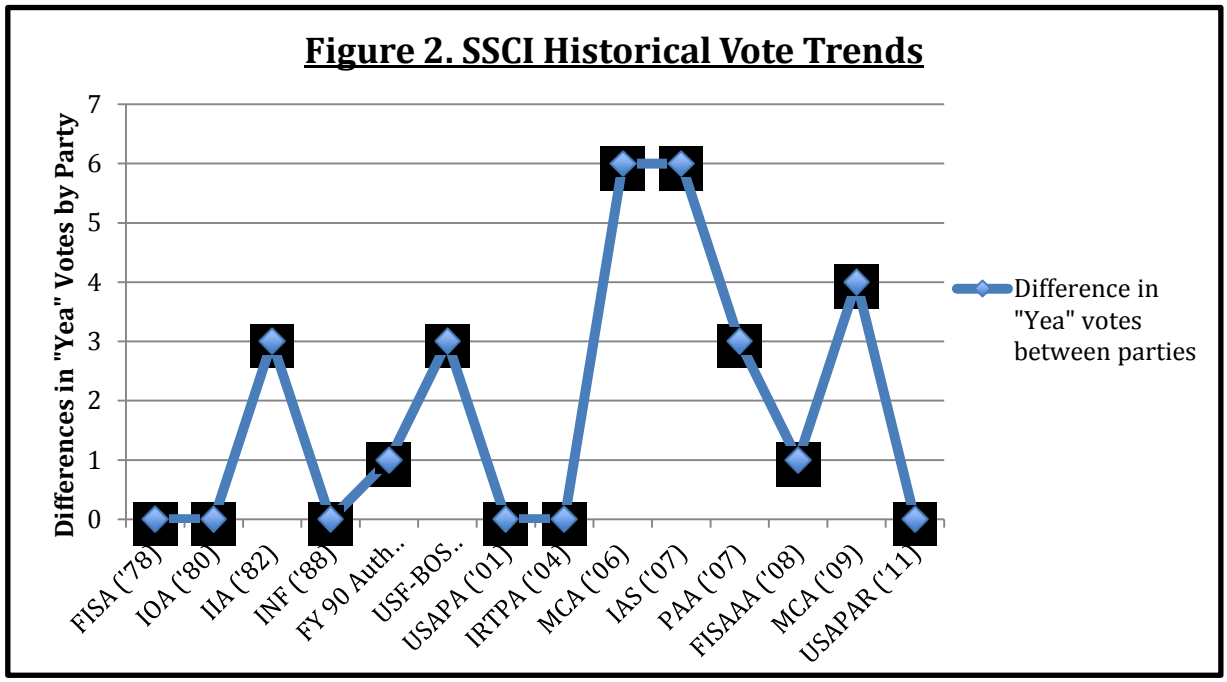
Figure 1. SSCI Partisan Representation



SSCI members were divided into four partisanship categories based on DW Nominate score. < -0.50 were considered strongly liberal, those > -0.50, but < 0 were considered moderately liberal, those > 0, but < 0.50 were considered moderately conservative, and finally members > 0.50 were considered strongly conservative.

into either the strongly liberal or strongly conservative categories. The increasing partisan membership trends on the SSCI were buttressed by reviewing voting trends on significant pieces of legislation throughout the SSCI's history.

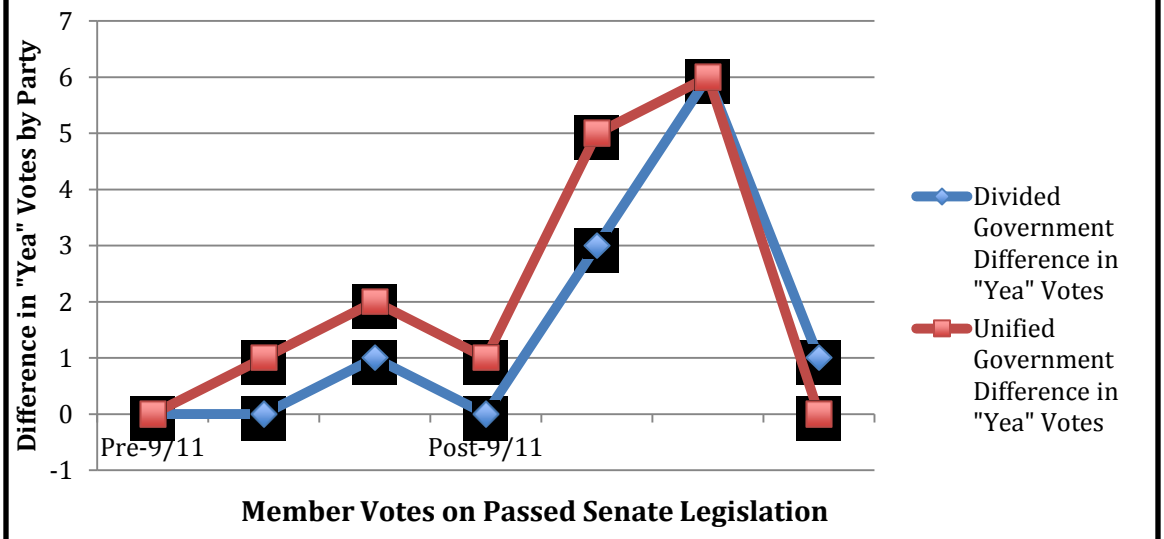
The fourteen pieces of intelligence or national security related legislation reviewed between 1978 and 2011 reinforce the idea of modestly increasing partisanship within the SSCI [Figure 2]. After the passage of IRTPA in 2004, the difference in "yea" votes between Democrats and Republicans rose significantly. Votes for Improving America's Security Act, the 2006, and 2009 Military Commissions Acts all contained "yea" vote differences greater than three votes. Members were more divided on each of these legislative actions than in earlier legislation. The other noteworthy aspect of the data is the greater fluctuations in "yea" vote differences since 2004. The "yea" vote differences do not consistently rise; rather they indicate that on certain legislation there is less likelihood members will cross party lines. Politically sensitive topics in the last ten



years garner greater party unity, but on issues with less salience or less political division SSCI members vote together. In addition, 2001 to 2004 likely contains heavy influence in the aftermath of 9/11 and a strong motivation for bipartisanship. There are no doubt other factors influential in "yea" or "nay" votes on legislation. However, a lack of SSCI cohesion on numerous pieces legislation suggests the possibility of persistently divided votes.

Figure 3 examines the influence of divided government on SSCI members' votes. Generally, periods of unified government led to increased differences in "yea" votes among SSCI members. One possibility is that during periods of undivided government the minority party unified along party lines in order to prevent the executive branch from achieving its objectives. This research considered SSCI members' votes on six pieces of legislation before the September 11th 2001 terrorist attacks and eight pieces of legislation after. Divided or unified, the latter time period included four Senate floor votes with large differences in "yea" votes among SSCI members. It reinforces the theory that

Figure 3. Divided Government Influence on Voting



partisanship in the SSCI is slowly increasing and rejects the supposition that periods of divided or undivided government substantially influence SSCI partisanship.

Rising partisan representation and rising divisions in voting trends supports scholarly opinion and suggests partisanship is increasing in the SSCI. Divided voting among SSCI members has some persistence over time, but when combined with greater partisan representation the SSCI's ability to provide effective IC oversight potentially diminishes. An interesting trend in the data occurs over the most recent decade as it reveals sporadically strong partisan voting. The next ten years in the SSCI will demand close attention as the upcoming decade might indicate whether representation and voting trends continue to rise at dramatic rates. One advantage to rising partisanship within SSCI ranks is the decreased likelihood the committee will suffer from any form of "regulatory capture." Despite this advantage, confirmation of increasing partisanship on the SSCI creates questions related to its ability to provide effective IC oversight and meet national security demands.

CONCLUSION

What it lacks in authority the SSCI makes up for in responsibility. It should be one of the least partisan committees in the Senate. The data suggests both political parties are increasing the percentage of strongly liberal or conservative members named to the SSCI. It also indicates SSCI members have always maintained some divisions in their voting trends regardless of divided government. One effect of increased committee partisanship is an increased probability that meaningful legislation will lack bipartisan support. A second consequence is the possibility the IC grows increasingly disillusioned with the SSCI and obstructs necessary oversight. The SSCI requires a strong relationship with the

IC so they remain informed of IC actions and needs. The IC and U.S. national security demand meaningful and effective support from the SSCI as the world rapidly evolves. Decentralized terrorist networks without state sponsorship, Internet related cyber threats to infrastructure from loosely state sponsored actors, and unstable authoritarian regimes that constantly provoke U.S. allies demand constant intelligence coverage. In conjunction with support to the IC, the SSCI must be capable of providing effective IC oversight to protect American civil liberties. It is imperative the SSCI is up to the task of providing well defined and timely legislative action to guide the IC.

CHAPTER TWO: THE CYBER DOMAIN- A CASE STUDY IN SSCI OVERSIGHT

Technological innovation in twentieth century America led the world and helped establish lone super power status for the United States (U.S.). This innovation contributed to military victories, scientific break-through, and provided personal computing power, as well as a globally networked web of computers. Twentieth century technological innovation in America touched every aspect of Americans' lives from their finances, to energy, to their sense of security. Pre-September 11, 2001, there was an overriding confidence military technology protected American shores from surprise attack. However, terrorism was not the only growing threat in the early twenty-first century. The rise of the Internet changed the way the IC conducted the day-to-day business of gathering foreign intelligence and preventing attacks against the U.S. It altered the threat matrix for the IC and exponentially increased the volume and geographical diversity of threats.

With congressional oversight responsibilities for the IC, the SSCI has an essential stake in the effectiveness of IC cyber domain activities. As part of the oversight process, the SSCI must ensure those programs conform to the democratic principles set forth in the American Constitution.[80] In the public arena, cyber domain debates (foreign or domestic) appear to be driven by leaked information or external events that spark public discourse, vice any anticipatory consideration of emerging cyber threats. Historically, the SSCI is reactionary to external revelations of IC abuses or failures and when investigating SSCI oversight in the cyber domain the evidence suggests the trend has

[80] For the purposes of this research the term cyber domain encompasses the interconnected nature of the Internet and the associated underlying information/telecommunications infrastructure. It is used loosely to evaluate the Intelligence Community's role in all forms of computer/telecommunications based foreign and domestically directed intelligence activities.

continued. A review of open hearings since 2004 suggests the SSCI has handled emerging cyber threats and the legality of employed IC cyber domain tactics, techniques, and procedures (TTPs) independently of one another. This case study presents original evidence gathered from open hearing testimony that the SSCI failed to overcome the topic du jour and offer forward thinking oversight to the IC on cyber domain issues. However, the study also uncovered qualitative strengths in SSCI oversight practices that address commonly held conceptions about IC oversight in the last decade.

AN IMPETUS FOR OVERSIGHT

The SSCI was born out of the ashes of a firestorm involving constitutional violations by the CIA and other prominent IC members. Reactive to governmental distrust caused by Watergate and Vietnam, Congress passed the Hughes-Ryan Amendment to the 1961 Foreign Assistance Act, but the amendment failed to curtail executive action without informing Congress. The 1974 series of New York Times articles by Seymour Hersh became an impetus for inquiry. Hersh disclosed the CIA's unauthorized intelligence collection targeting thousands of Americans along with other violations of the 1947, National Security Act.[81] By 1975 both chambers of Congress and the White House were clamoring to establish IC investigative committees; the Senate's answer was the Church Committee.[82] Through its investigation, the Church Committee identified a variety of instances where IC members violated the rights of Americans. For 18 years the CIA

[81] As described in Loch Johnson's *A Season of Inquiry*, then DCI James Schlesinger compiled the CIA's 'family jewels' in 1973 in order to understand the possible range of CIA violations. In total Schlesinger was provided approximately 700 violations, some of which were eventually leaked to Seymour Hersh.
[82] Loch K. Johnson, *A Season of Inquiry: Congress and Intelligence*, (Chicago: Dorsey, 1988): 9-11. Johnson noted "[t]he newly elected members of Congress in 1974 (the aggressive post-Watergate class) included a large number who had won office by campaigning against the imperial presidency of Richard Nixon and promising a new morality in government. At the first hint of CIA domestic abuses—hardly a month after their election—these new members rose together in loud indignation, demanding a full inquiry" (pg. 11).

operated HT Lingual, a mail-opening program targeting Americans who sent or received mail from communist countries. In addition, the CIA initiated OPERATION CHAOS, collecting intelligence on student protestors across the U.S.: directly violating the CIA's original charter.[83]

Domestic intelligence agencies, including the FBI gathered information on political activists from the IRS Special Services Staff. One of the more spectacular discoveries was FBI use of IRS data in an attempt to disrupt the fund-raising program of Dr. Martin Luther King Jr's Southern Christian Leadership Conference (SCLC).[84] The FBI also operated the Counterintelligence Program (COINTELPRO), aimed at suppressing dissenters from all walks of society.[85] Under the auspices of COINTELPRO, the FBI claimed Dr. Martin Luther King Jr. was a national security risk and attempted to subliminally convince Dr. King to commit suicide through anonymous letters describing apparent extramarital affairs.[86] In all, approximately 2,000 women's liberation activists, white supremacists, anti-war protestors, and left-leaning socialites were all subject to FBI surveillance and harassment. The enormity of the IC abuses cannot be overstated and in spite of significant political obstacles the Senate established the SSCI in 1976.[87] Thirty

[83] Ibid., 82 & 85-87.
[84] Ibid., 91.
[85] Loch Johnson's *A Season of Inquiry* describes in detail on page 129 statements regarding COINTELPRO by Senator Philip Hart, who was in poor health at the time of the hearings. Hart was attending his first hearings of the investigation and recounted his past defense of the intelligence community to family members who believed the FBI had tried to discredit Vietnam dissenters in Michigan. Johnson quoted Hart as saying, "[w]hat you have described is a series of illegal actions intended to deny certain citizens their First Amendment rights— just like my children said."
[86] Ibid., 127-128.
[87] For greater insight into the political obstacles facing SSCI establishment see Chapters 20 and 21, of *A Season of Inquiry* by Loch Johnson. The language of Senate Resolution 400 faced opposition by Rules Committee Chairman Howard Cannon (D-Nev) who desired further study regarding the establishment of a permanent intelligence oversight committee, as well as by the Judiciary Committee and the Armed Services Committee, neither of which wanted to see their historic jurisdiction infringed upon.

years of SSCI oversight set against the historical tapestry of those violations lays the foundation for analyzing SSCI oversight in the cyber domain.

EFFECTIVENESS OVER TIME

At the conclusion of a 34-year CIA career, former Acting General Council, John Rizzo characterized communication challenges as the most significant failure in the relationship between Congress and the CIA.[88] The agency consistently struggled to determine what information to report to the SSCI and when to report it.[89] Rizzo's sentiment highlights a lack of strategic guidance to the IC, which the SSCI has oft struggled to provide. Considerable scholarship argues rising ideological divisions and partisanship jeopardizes effective IC oversight.[90] Despite a history of bipartisan cooperation, fractured budgetary authority and an increasing lack of IC familiarity have challenged the SSCI.[91] These two institutional shortcomings are well documented in scholarly literature and will not be reinvestigated in an effort to specifically address cyber domain oversight.

Throughout its history individual SSCI members have adopted different approaches to IC oversight. Some members neglect oversight of the IC, other members champion the IC without fail, while still other SSCI members eye the IC with skepticism. Finally, some members choose a balanced approach between championing the IC's

[88] John Rizzo, "The CIA-Congress War," *Defining Ideas* (2012): http://www.hoover.org/publications/defining-ideas/article/112491 (accessed 15 June 2013).
[89] Rizzo continued his explanation of communication challenges with the SSCI by noting the CIA was, "operating under frustratingly ambiguous standards imposed on the Agency by a Congress that has grown ever more suspicious of CIA's motives and commitment to the oversight process."
[90] Matthew B Walker, "Reforming Congressional Oversight of U. S. Intelligence," *International Journal of Intelligence and Counterintelligence* 19 no.4 (2007): 704-706.
[91] Amy Zegart, *Eyes on Spies: Congress and the United States Intelligence Community*, (California: Hoover Institution Press, 2011), 10-11.

purpose while closely monitoring its activities.[92] Collectively, the SSCI has approached IC oversight through the leadership and impulses of its chairmen. Whether led by Senator Boren (D-Oklahoma) or Senator Shelby (R-Alabama) the SSCI has largely conformed to the prosecutorial or cooperative relationships of SSCI chairmen.[93] Disparate individual approaches to IC oversight combined with the paradigms of its various chairmen both contribute inconsistency.[94] Rising partisanship aside, the SSCI has had successes and failures worth examining that are directly connected with future oversight in the cyber domain.[[95]][[96]] Its recent history suggested a case study would help evaluate oversight in the cyber domain by analyzing the triumphs and faults. Ultimately, the committee has strived to triangulate the provision of effective intelligence oversight while protecting national security and defending the constitutional civil liberties

[92] Loch K Johnson, "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability," *Intelligence and National Security* 23 no.2 (2008): 199. Johnson categorizes the four groups as the ostriches, the cheerleaders, the lemon-suckers, and the guardians.

[93] L. Britt Snider, *The Agency and the Hill : CIA's Relationship with Congress*, 1946-2004, (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2008), 83. According to Snider, Senator Boren was an exemplar of effective oversight and bipartisanship. "Boren believed that partisanship in matters of national security should stop at the water's edge...Boren served as SSCI chairman for six years, allowing him to compile a record of legislative achievement unmatched by any of his predecessors…Boren's achievements owed much to his talent (and his penchant) for consensus building and helped him hold the chair for six years." In contrast Snider also noted the nature of Senator Shelby's chairmanship, which was marked with high profile and partisan investigations into Clinton's nomination of Anthony Lake as DCI, the accidental bombing of the Chinese embassy in Belgrade, and the 1998 Indian nuclear tests.

[94] Loch Johnson notes on page 210 in "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability," that as crises have occurred since 1975 lawmakers have responded well as "fire-fighters" to alarms and fires, but have failed to effectively patrol the IC in day-to-day oversight.

[95] In *Eyes on Spies*, Amy Zegart adds credibility to the arguments in support of inconsistent oversight by offering quantitative evidence of fewer SSCI hearings and legislative action as compared to other Senate oversight bodies.

[96] Frank J. Smist, *Congress Oversees the United States Intelligence Community, 1947-1993*. 2nd ed (Knoxville: The University of Tennessee Press, 1994), 126. The 1978 Foreign Intelligence Surveillance Act first established judicial review of intelligence operations. This watershed legislation and its subsequent amendments relate directly to some of the oversight challenges in the cyber domain. The Foreign Intelligence Surveillance Court is responsible for authorizing electronic surveillance within the U.S. Twenty-first century telecommunications and the Internet age has blurred national boundaries and engendered questions regarding the legislation's relevancy.

of all American citizens. However, as the cyber domain increases in complexity the SSCI must better anticipate the needs of the IC.

THE VENERABLE CYBER DOMAIN

In 2010, Vice Admiral (Ret) Mike McConnell wrote that the U.S. was engaged in a cyber war and losing. He went on to suggest the U.S. lacked a cohesive cyber defense strategy. McConnell highlighted the U.S. government and public's reliance on information and telecommunications networks, and proposed that the current cyber war had the same economic and psychological importance as the nuclear challenge during the Cold War.[97] However, concerns regarding the cyber domain are not as recent as 2010 and actually reach back to the 1960s.

As far back as the 1960s NSA officials and policymakers were aware of the significant vulnerabilities associated with classified information residing on shared computer systems.[98] Throughout the 1970's computer security improvements included hashed passwords, file system permissions, administrator privileges, and the introduction of computer encryption by IBM.[99] There was no shortage of government interest with respect to emerging communication and network technology leading into the 1980s and 1990s.[100] The idea of data integrity promulgated throughout the 1980s and spread in

---

[97] Mike McConnell, "Mike McConnell on How to Win the Cyber War We are Losing," The Washington Post (February 28, 2010). Vice Admiral McConnell (Ret) is the former Director of NSA and former Director of National Intelligence.

[98] Michael Warner, "Cyber Security: A Pre-History," *Intelligence and National Security* 27 no.5 (2012): 783-785. Warner suggests that in the 1960s policymakers were aware of the possibility that data could spill. In the 1970s policymakers gain an appreciation for data theft and computer attack. In the 1980s and 1990s the government began incorporating cyber warfare in military planning. And in the 1990s policymakers also began to worry about computer-based attacks emanating from foreign adversaries.

[99] Ibid.

[100] In 1986 Congress passed the Stored Communications Act as part of the Electronic Communications Privacy Act. The SCA addresses the privacy of stored communications and sets the threshold the government must meet to compel the content of certain Internet communications. For additional information on the ECPA and SCA see Orrin Kerr's, "A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It," published in 2004.

conjunction with military information warfare doctrine into the 1990s.[101] By 1997 the President's Commission on Critical Infrastructure Protection (PCCIP) characterized many of the same challenges associated with the cyber domain the U.S. faces today. The PCCIP identified gaps in security, obstacles to accurate origin and attribution, and ever expanding accessibility.[102] At the century's turn policymakers and legislators struggled to address security and privacy challenges they knew existed for almost thirty years.

Throughout this cyber history the IC has played a significant role in protecting sensitive information, defending information networks, and executing cyber operations targeting U.S. adversaries. In March 1998, malicious actors breached Department of Defense (DOD) and National Aeronautics and Space Administration (NASA) networks, stealing technical research, contracting information, encryption techniques, and inserting "back doors" for access later.[103] Today, DOD and IC networks are targeted daily, leaving sensitive data vulnerable if detection and prevention systems are not constantly advancing.

While testifying before the SSCI in March 2013, Director of National Intelligence (DNI) James R. Clapper opened his remarks by highlighting recent cyber attacks that had directly targeted critical infrastructure systems.[104] These types of attacks exemplify the growing intersection between the private sector and the IC in the cyber arena. For

---

[101] Ibid., 786 & 790-791.
[102] James Ellis, David Fisher, Thomas Longstaff, Linda Pesante and Richard Pethia, *Report to the President's Commission on Critical Infrastructure Protection*, (Pittsburgh: Carnegie Mellon University, 1997).
[103] James Adams, "Virtual Defense," *Foreign Affairs* 80 no.3 (2001): 99-100. The attack against American networks purportedly emanated from Russia and is known within the IC as MOONLIGHT MAZE.
[104] James R. Clapper, *"Worldwide Threat Assessment of the U.S. Intelligence Community,"* Statement for the Record, Senate Select Committee on Intelligence (Washington D.C., March 12, 2013). DNI Clapper's examples took place in 2012 when private U.S. banks and stock exchanges were victims of denial-of-service attacks while the Saudi Oil Company Aramco was targeted with malicious software that rendered 30,000 company computers inoperable.

example, in 2010, 90 percent of the physical infrastructure for the Internet was owned by private industry.[105] The IC is forced to engage and communicate with the private sector because the underlying infrastructure of the Internet resides outside IC control.[106] Cyber threats over the last ten years progressed through the voluminous increase in the variety of Internet based tools, the complexity of the environment, and an expansion of adversaries.

Cyber attacks conducted in 2007 and 2008 by possible Russian proxy elements against the governments of Georgia and Estonia exemplified the expanding options for denial of service attacks to make political statements or support military operations.[107] In 2008, the NY Times reported on cyber attacks targeting the Iranian nuclear program, most likely executed by the U.S. and Israel. The cyber weapon known as 'Stuxnet' successfully destroyed Iranian centrifuges and exploited vulnerabilities within physical infrastructure systems.[108]

In the twenty-first century threats no longer only emanate from nation-states and this shifting threat landscape places IC resources at a premium.[109] Adversaries in the

---

[105] McConnell, "Mike McConnell on How to Win the Cyber War We are Losing."

[106] According to Hughes and Stoddart's, "Hope and Fear: Intelligence and Global Security a Decade After 9/11," *Intelligence and National Security* 27 no.5, in FY 2005, 70 percent of the intelligence budget was spent in the private sector; another contributing factor among many for the increasing complexity of the cyber operating environment.

[107] Sanjay Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence," *Communications of the ACM* 54 no.8 (2011): 135. The cyber attacks mounted in Estonia were in response to the Estonian Governments decision to remove a Russian WWII memorial. In Georgia the denial of service attacks disrupted the government's ability to communicate with their citizens during military conflict with Russia. Both were viewed as attacks that at least had tacit approval by the Russian government.

[108] Eric Lorber, "Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?," *University of Pennsylvania Journal of Constitutional Law* 15 no.3 (2013): 971.

[109] Hughes and Stoddart also note, "thanks to the rapid advances in global communications, any action, inaction or failure on the part of the intelligence agencies can potentially be exposed instantaneously to a global audience. This necessarily affects the 'nature of the product itself, but also the means of procurement and analysis, and the organizations that deal with it'. Given diminishing resources brought about by the global economic downturn, intelligence organizations are increasingly under pressure to successfully map out priorities in advance of events. These priorities encompass both traditional security

cyber domain share common attributes with terrorist groups who are smaller and more agile. Globalization has facilitated the easy movement of weapons, people, information, and other materials across national borders. For the IC, the complexity and uncertainty surrounding threats increases while the protection provided by natural geographic barriers diminishes.[110] As geographic boundaries become less relevant the importance of effective oversight and prioritization by policymakers and legislators becomes more important.[111] It is not always apparent when constitutionally protected rights might be infringed upon by an IC working diligently to protect those very freedoms. While the security and privacy difficulties associated with the cyber domain are long since documented the solutions are more challenging to find.

OVERSIGHT MODELS & THE 'BOTTOM LINE UP FRONT'

Existing theory implies broadly dysfunctional IC oversight by the SSCI.[112] A disciplined configurative analysis of cyber oversight using controlled comparison case studies offered the best opportunity to derive theoretical generalizations on overall SSCI effectiveness.[113] Dr. Amy Zegart's four-component model for effective oversight supplied independent variables for studying the underlying dysfunction oversight

---

challenges as well as increasingly complex and inter-connected non-traditional problems (pg. 633)." They go on to quote DCI Porter Goss testifying before the Senate and saying, "we need to make tough decisions about which haystacks deserve to be scrutinized for the needles that can hurt us most. And we know in this information age that there are endless haystacks everywhere."

[110] Myrium D. Cavelty and Victor Mauer, "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence," *Strategic Dialogue* 40 (2009): 127-128.

[111] Consider that during the Cold War the adversary was easily identifiable, but difficult to eliminate. However, in the 21st century the adversary might be a U.S. citizen logged into a Yahoo account at an Internet café in a third party country and transmitting malicious code through the servers of U.S. companies.

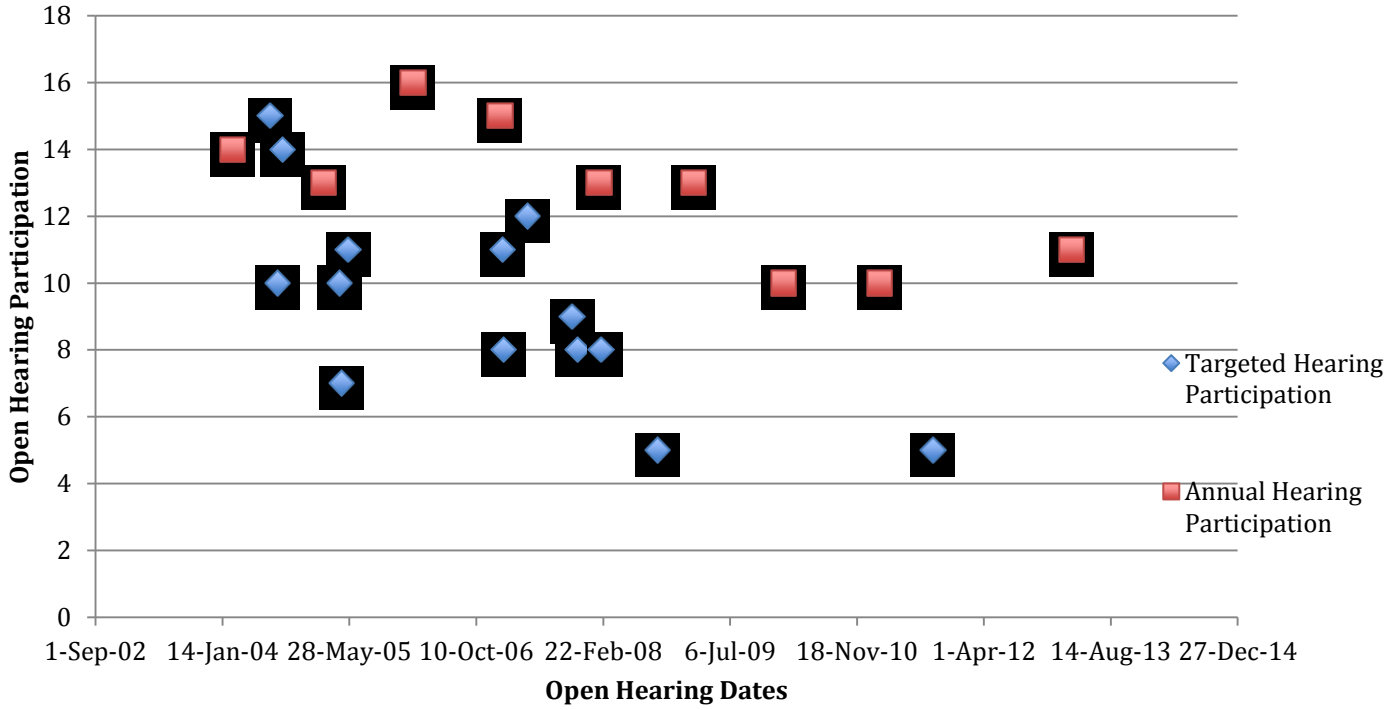
[112] Both academic literature, as well as the 9/11 Commission highlights IC oversight dysfunction.

[113] Alexander L. George, "Case Studies and Theory Development: The Method of Structured, Focused Comparison," In *Diplomacy: New Approaches in History, Theory, and Policy,* edited by Paul Gordon Lauren, (New York: The Free Press, 1979), 50-51. George describes on page 50 that a disciplined configurative mode of analysis "employs general variables for the purposes of description and explanation."

supposition.[114] Zegart's model fit a disciplined configurative mode of analysis, where effective oversight was dependent on constitutional adherence, strategic guidance, legislative activism, and public advocacy. Open hearings over the last ten years offered considerable material to assess SSCI oversight effectiveness in the cyber domain based on the four independent variables.

Zegart describes the four functions of effective IC oversight by Congress as 1) the

Figure 4. Open Hearing Participation



Targeted hearing participation tracks committee member participation in hearings focused on unique intelligence oversight topics. Annual hearing participation identifies member participation in annually held open hearings on national security threats facing the U.S.

policeman, 2) the board of directors, 3) the coach and, 4) the ambassador.[115] First, the SSCI's oversight responsibilities include monitoring IC cyber activities for constitutional

[114] Zegart, *Eyes on Spies: Congress and the United States Intelligence Community*, 31.
[115] Ibid.

adherence. The committee has a police-patrol function to perform by ensuring the IC operates within the left and right limits of the law. Second, in order to provide effective oversight the committee must offer strategic guidance to the IC as it sets priorities for cyber operations. Third, the SSCI cannot provide effective oversight without investigation and activism. The committee must proactively study IC cyber programs to ensure they are effective and efficient. Finally, the SSCI has an important role in educating the public on the significance and legality of IC cyber operations. The SSCI's public advocacy responsibilities provide the public reassurance oversight is conducted properly.[116]

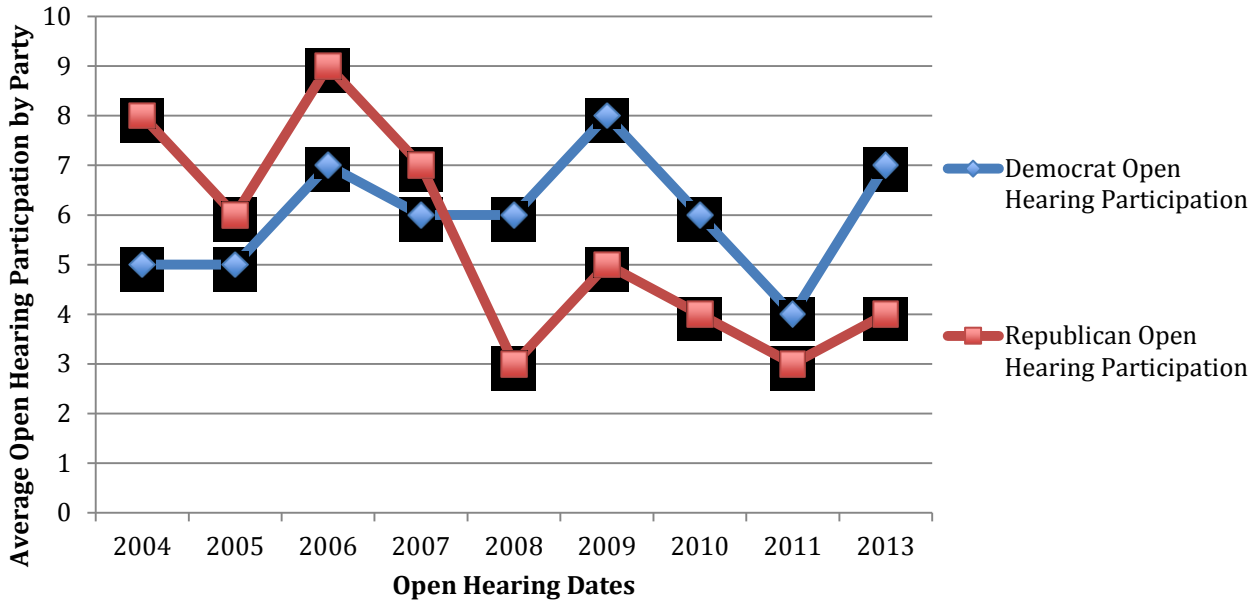
In selecting appropriate cases to evaluate the committee's execution of the these four responsibilities it was important to gather from annual hearings where IC leaders presented information regarding the current threats facing the U.S. and specialized hearings where the IC provided descriptive accounts of cyber domain operations. One of the shortcomings in this research was the inability to analyze all SSCI hearings over ten years. This research only reviewed open hearings conducted by the SSCI, however given the committee's public advocacy role in providing effective oversight, the most useful material for analyzing that oversight was publically available. Only a fraction of total hearings were available in the public record, but those open hearings had continuity as annual events, as well as specialized focus on issues most relevant to IC cyber operations. The open hearings offered a clear framework for analysis and did not substantially degrade the validity of the findings.

In order to draw conclusions from the case studies it was necessary to briefly analyze the hearings quantitatively and ensure sufficient member and party participation.

[116] Ibid.

Figure 4 depicts hearing participation by SSCI members over the last ten years. Annual and targeted hearing participation declined during this time period, although the declines were more pronounced in targeted hearings. Despite several outliers however, the committee consistently garnered at least 50 percent participation from SSCI members during open hearings. In addition, annual threat hearing participation remained above 65 percent for each year studied. Figure 5 demonstrates open hearing participation based on party and a shift in hearing participation based on the party in control of the Senate. Both parties averaged approximately 5 members at all of the open hearings researched in this study. Through the end of 2006 Republican Party committee members often had greater hearing participation. This shifted to Democratic Party members as they took control of the Senate in 2007. However, because hearing participation followed this pattern over the course of ten years the open hearings provided equal opportunity for both parties to be active in cyber oversight. Neither party completely dominated the cyber oversight debate. Additionally, Appendices 2 and 3 depict the timeline of open hearings and offer bulleted summaries of cyber oversight activities.

Figure 5. Party Particpation in Open Hearings



In years where multiple hearings took place member participation is averaged to the nearest whole number.

The significance of cyber oversight required no further research beyond the front page of major U.S. newspapers in mid-2013. On June 5th, 2013 Glenn Greenwald published an article in *The Guardian Newspaper* exposing a FISA court order for Verizon Communications to provide the FBI and NSA bulk call transactional data over the course of three months.[117] Subsequent articles in *The Washington Post* and *The Wall Street Journal* detailed court orders and information sharing agreements between telecommunications firms and Internet service providers.[[118]][[119]] These relationships

[117] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, (June 5, 2013). Greenwald noted in his article FISA court orders are traditionally granted for a specific individual or target, not mass amounts of data for long periods of time.
[118] Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, (June 6, 2013). The Washington Post identified a program known as PRISM that was initiated following the 2007 FISA amendments known as

highlighted the importance of oversight in the ongoing attempt to balance national security and civil liberties. Following the articles, officials rushed to assuage public fears and highlight that all three branches of government had approved the measures in place.[120] Nevertheless, the most significant issue remains unanswered; when it comes to intelligence gathering, how much freedom should the IC be given to execute its missions?

The SSCI's oversight role for the IC extends beyond simple constitutional adherence and requires the committee provide strategic guidance, public advocacy, and legislative activism. Effective congressional oversight contributes to a healthy debate for future IC cyber activities as policymakers and the public gain a better understanding of the cyber domain. The SSCI should lead discussion regarding the legal framework for domestic and foreign IC cyber operations. Evaluating the committee's effectiveness in all four components of oversight during annual threat briefings provided nuanced insights into its approach to cyber oversight.

CURRENT & PROJECTED THREATS TO NATIONAL SECURITY

In the last ten years the SSCI has slowly developed the appetite to discuss national security implications in the cyber domain. On an annual basis, the SSCI conducts open hearings to explore emerging threats to the United States. On the legality of electronic

---

the Protect America Act. It is note worthy that SSCI members voted 11 yeas to 4 nays in support of the legislation when it passed on the Senate floor. The four nay votes came from Senators Feingold, Rockefeller, Wyden, and Whitehouse. According to the Washington Post, PRISM latched 9 Internet services providers with IC agencies to gather data off private servers.

[119] Siobahn Gorman, Evan Perez, and Janet Hook, "U.S. Collects Vast Data Trove," *The Wall Street Journal*, (June 7, 2013).

[120] In a July 2013 letter to Senator Wyden, DNI Clapper provided a timeline of informative briefings the IC provided to the SSCI and other members of Congress with respect to USA PATRIOT Act Section 215 authorities. According to DNI Clapper, Section 215 authorized the collection of bulk telephony meta-data, specifically origination data, telephone numbers, duration, and receiver information. He highlighted call content was not collected and provided answers to questions posed by 26 U.S. Senators. Also noteworthy, the letter indicated the NSA was authorized under these authorities to collect bulk Internet meta-data. The letter is available at <http://www.wyden.senate.gov/download/?id=87b45794-0fa4-4b1a-b3a6-e659a91a5042>

surveillance and issues related to the FISA the SSCI has shown some consistency in open hearings. However, on foreign focused operational matters related the cyber domain, the SSCI has only started to address the issue in open hearings in the last five years. From 2004 to 2008, cyber security, cyber threats, and cyber operations were largely absent from SSCI hearings. The makeshift approach to ensuring constitutional adherence, promoting public knowledge, offering strategic guidance, and proactively investigating cyber programs is evident in the record.

In 2004 and 2005, testimony regarding foreign-based cyber threats facing the nation was sparse and rarely did SSCI members respond with questions related to the cyber domain. In 2004 and 2005 open hearings, FBI Director Robert Mueller noted the cyber threat as one of the top three growing threats to the nation and emphasized improved IC information sharing as a result of FISA court rulings and the USA PATRIOT Act.[121] Most importantly, in 2004 Director Mueller suggested to Senator Dianne Feinstein (D-California) the need for legislation addressing private companies who support terrorist investigations.[122] The preponderance of discussion in open hearings during those years centered around proliferation, terrorism, geographically based threats, and Iraq WMD, while the SSCI failed to meaningfully address IC cyber operations in response to emerging threats.

In 2005, the only Senator questioning the constitutional adherence of IC operations in the cyber domain was Senator Ron Wyden (D-Oregon). Senator Wyden requested the IC explain the rules governing data mining and collection of information on

[121] Senate Select Committee on Intelligence, *Current and Projected National Security Threats to the United States* S. Hrg 108-588 (Washington: U.S. Government Printing Office, 2004), 5, 38, & 92-93.
[122] Ibid.

American citizens.[123] While Senator Saxby Chambliss (R-Georgia) highlighted the importance of the USA PATRIOT Act, the rest of the committee took no opportunities to publically proclaim or vilify the significance of IC cyber engagement.[124] The issues identified in open hearings through 2008 regarding the intersection of the IC and the cyber domain were procedural and domestically focused. Foreign based cyber threats or U.S. capabilities in the cyber domain went unaddressed.

The domestic legal narrative surrounding the IC in the cyber realm expanded in 2006 and 2007 where a considerable portion of the discussion was politically driven banter regarding NSA warrantless wiretapping of Americans.[125] In 2006, Senator Wyden revisited the topic of data mining rules and regulations, while other Democratic committee members lamented the Executive Branch's unwillingness to keep the SSCI informed.[126] 2007 provided similar, but less abrasive dialogue regarding IC involvement in the cyber realm.[127] This type of oversight failed to address the underlying implications of warrantless wiretapping and data mining. The constitutional adherence and public advocacy elements of oversight were in effect without the legislative activism or strategic guidance to provide the IC clear boundaries as it utilized an emerging collection platform.

---

[123] Senate Select Committee on Intelligence, *Current and Projected National Security Threats to the United States* S. Hrg 109-61 (Washington: U.S. Government Printing Office, 2005), 92-94. Senator Wyden readdressed the issue in 2006 after providing the IC a year to gather the requisite information. He further expressed concerns the IC lacked rules and regulations to govern cyber domain actions.

[124] Ibid., 64-65.

[125] Senate Select Committee on Intelligence, *Current and Projected National Security Threats to the United States* S. Hrg 109-724 (Washington: U.S. Government Printing Office, 2006), 6-7 & 50-68.

[126] In 2006, Senator's Rockefeller, Feingold, Feinstein and Carl Levin (D-Michigan) all used the opportunity to question the legality of NSA's wiretapping program when only 4 out 535 members of congress were informed on the details of the program. Additionally, the 1991 Intelligence Authorization Act requires the president to keep the SSCI currently informed of foreign directed covert actions. However, in the case of warrantless wiretapping the program was domestically focused and a select few congressional leaders were informed.

[127] Senate Select Committee on Intelligence, *Current and Projected National Security Threats to the United States* S. Hrg 110-835 (Washington: U.S. Government Printing Office, 2007), 3 & 53-54.

The questions being addressed in 2013 are not new, but unresolved oversight debates from the last the decade.

For the first time in 2008 the SSCI began to address the foreign operational issues associated with IC involvement in the cyber domain. In his opening remarks, SSCI Chairman John D. Rockefeller IV (D-West Virginia) noted,

> [t]hreats can come in unfamiliar ways. And because our society is very complex, we are vulnerable to threats we may not fully appreciate. In this regard, I'm very concerned about the potential of cyberattacks—they have already been executed—and our ability to protect our critical infrastructure. This is something we have discussed before. Cybersecurity is a growing subject of importance that will be addressed by the committee in detail, intensely, in the coming weeks.[128]

Senator Rockefeller's statement reflects the improving public advocacy dimension of cyber oversight in SSCI dialogue regarding both domestic legal issues and foreign operational matters. This was the first hearing where cyber threats were associated with foreign adversaries.[129] Vice Chairman Christopher Bond (R-Missouri), Senator Orrin Hatch (R-Utah) and Senator Mark Warner (D-Virginia), all emphasized the need for a strong public/private partnership to address emerging challenges in the cyber domain.

At the forefront of their discussion points was an emphasis on the need for liability protection for companies who partner with the government regarding cyber issues.[130] SSCI members announced support for FISA renewal in order to continue engagement with the private sector, but reinforced inconsistent strategic guidance. In subsequent years private sector engagement was emphasized continually to address

---

[128] Senate Select Committee on Intelligence, *Current and Projected National Security Threats to the United States* S. Hrg 110-824 (Washington: U.S. Government Printing Office, 2008), 3.
[129] Russia and China were identified during discussion as well as through written questions as cyber actors requiring attention.
[130] Ibid., 72, 86, & 92. This particular liability protection was to protect companies who provided information to the government as a result of a FISA order.

foreign intelligence operational issues in the cyber domain. Simultaneously, the legal underpinnings of domestic surveillance programs were hotly contested, but also required private sector engagement in an effort to prevent terrorist attacks.

In its annual opening hearings regarding threats to national security over the last five years, the SSCI has covered the complexity of cyber threats, vulnerabilities of U.S. information technology systems, and emerging foreign cyber adversaries at length. The 2009 hearing included discussion regarding the cyber threat posed by Russia and China, as well as the vulnerability of the U.S. power grid to cyber attack.[131] Senator Feinstein suggested an important component to the international legal framework for cyber policy was a diplomatic initiative to establish a cyber code of conduct.[132] 2009 was also the first hearing in which the challenges associated with cyber security were addressed in conjunction with the protection of civil liberties and privacy.[133] The SSCI demonstrated some legislative activism by conducting five hearings related to cyber security in 2009 and establishing a three-member task force to review cyber plans.[134]

In 2010 and 2011 two open hearings reinforced the magnitude and diversification of the cyber threat. Unfortunately, those hearings failed to build on Senator Sheldon Whitehouse's (D-Rhode Island) suggestion that oversight dialogue needed to envelope cyber security with civil liberties.[135] The emphasis from committee members was on malicious code, loss of revenue in the financial sector, and the role of the private

[131] Senate Select Committee on Intelligence, *Current and Projected National Security Threats to the United States* S. Hrg 111-62 (Washington: U.S. Government Printing Office, 2009), 60 & 74.
[132] Ibid.
[133] Ibid., 78. Senator Whitehouse questioned how to safely engage in a dialogue concern both cyber security and civil liberties in order to maintain public confidence in the IC's activities.
[134] Senate Select Committee on Intelligence, *Current and Projected National Security Threats to the United States* S. Hrg 111-557 (Washington: U.S. Government Printing Office, 2010), 2-3.
[135] *Current and Projected National Security Threats to the United States* S. Hrg 111-62, 78.

sector.[136] This foreign cyber threat dialogue continued a trend away from earlier years where the domestic cyber issues surrounding the IC were often discussed in conjunction with terrorism prevention.

Moving from rhetoric towards action, recommendations for legislative initiatives came from various SSCI members during the 2013 open threat hearing. Senator Dan Coats (R-Indiana) addressed the need for legislation that increased information sharing between the public and private sector. Senator Susan Collins (R-Maine) echoed that sentiment while expressing reservations about IC actions based on executive order. Chairman Feinstein expressed her and Vice Chairman Chambliss' determination to move cyber legislation through the SSCI in order to improve information sharing with the private sector.[[137]][[138]]

Despite late moves towards greater legislative activism and review of IC constitutional adherence by the SSCI, the evidence over the last ten years of annual threat hearings still suggests an inconsistent approach to cyber oversight. The SSCI's cyber oversight largely encompassed public advocacy. Whether focused domestically or on foreign threats there were few policy recommendations set forth during open hearings. In addition, for the entirety of the analysis there was a collective failure to acknowledge the

---

[136] Senate Select Committee on Intelligence, "Current and Projected National Security Threats to the United States," Hearing before the Select Committee on Intelligence of the United States Senate held on February 16, 2011, <http://congressional.proquest.com/congressional/docview/t65.d40.02160003.s32?accountid=11752> (accessed 7 July 2013).

[137] Senate Select Committee on Intelligence. "Current and Projected National Security Threats to the United States." Hearing before the Select Committee on Intelligence of the United States Senate held on March 12, 2013. <http://congressional.proquest.com.proxy3.library.jhu.edu/congressional/docview/t65.d40.03120003.s37?accountid=11752> (accessed 7 July 2013).

[138] Between 2010 and 2013, SSCI member rhetoric did not result in legislative action. According to Govtrack.us (https://www.govtrack.us/congress/bills/browse#congress=112&committees=2665), in 2012 and 2013, Representative Mike Rogers, Chairmen of the HPSCI introduced cyber related legislation, but in the 112th Congress SSCI members took no action related to the bill and it remains to be seen if SSCI members will take any action in the 113th Congress.

interconnection between the cyber issues of a domestic nature and those emanating from foreign adversaries. The SSCI separately emphasized and analyzed those issues during different time periods. The result of this shortfall was a significant gap in strategic guidance offered to the IC for the expanse of cyber related issues. It was important however, to also consider SSCI actions in targeted open hearings during the same time period and evaluate whether members provided more effective oversight on alternate topics.

TARGETED OPEN HEARINGS

Intelligence Reform. In the last ten years the SSCI devoted considerable time to investigating IC reform. Following recommendations for reform from the 9/11 commission and spurned by the mistakes made in Iraq WMD assessments, the SSCI was a key institution during the reform process in 2004, 2007 and 2011. However, the review of five open hearings on intelligence reform reinforces conclusions drawn from annual threat hearings. There was a lack of consistency in cyber domain oversight during IC reform dialogue. The cyber domain should have been a high priority issue for the SSCI in IC reform.

During the open hearing process in 2004 the committee and its witnesses stressed the urgency for action in creating the Director of National Intelligence (DNI) to remedy IC failures on 9/11 and in the Iraq National Intelligence Estimate (NIE). The primary focus for committee members was the roles and responsibilities of a new DNI, largely as a solution to terrorist threats.[[139]][[140]] The importance of a national counterterrorism

[139] Senate Select Committee on Intelligence, *Reform of the United States Intelligence Community* S. Hrg 108-835 (Washington: U.S. Government Printing Office, 2004), 34-36, 40 & 83-85. Dr. Amy Zegart and Dr. David Kay both testified to the unique opportunity for structural reform and the need to act quickly well the political will for change existed. The SSCI Chairman and Vice Chairman, Senators Bond, DeWine, and

center to unify IC efforts was also central concern.[141] Two years after Intelligence Reform and Terrorism Prevention Act (IRTPA) enactment, SSCI members took stock of the reform process, focused on the leadership of the DNI, and addressed reform at the agency level. SSCI members questioned the ODNI, FBI, and DHS on specific reform measures.[142] The committee also examined information sharing channels resulting from structural changes to the IC.[143] It was not until 2011 during review of IC reform in a joint setting that the issue of cyber domain oversight finally emerged as a topic of interest.[144]

As far back as 2004, SSCI members had opportunities to address the cyber domain during the intelligence reform process and failed to do so. In Vice Chairman Rockefeller's, 7 September 2004 opening statement he expressed the need to merge foreign and domestic efforts in counterterrorism through a national counterterrorism center.[145] In the same hearing Rockefeller highlighted the oft-minimal allegiance

---

Snowe all addressed considerations regarding a new intelligence director and his role in prevent intelligence shortfalls seen on 9/11 or in the Iraq WMD issues.

[140] Senate Select Committee on Intelligence, *Intelligence Community Reform* S. Hrg 108-656 (Washington: U.S. Government Printing Office, 2004). On page 3 of the hearing transcripts Chairman Roberts referenced the need for additional tools to handle the increasing volume of data being collected, but gave no further details regarding the nature of that data or how the IC was utilizing the data.

[141] Ibid., 67, 83, 85, 90. The SSCI Chairman, Pat Roberts and Vice Chairman Rockefeller emphasized the creation of a national counterterrorism center. The Vice Chairman of the 9/11 Commission in his opening statement reinforced this idea.

[142] Senate Select Committee on Intelligence, *Intelligence Reform* S. Hrg 110-839 (Washington: U.S. Government Printing Office, 2007), 9, 77, & 85. Witnesses during these two hearings included the Deputy Director for National Intelligence for Collection, Mr. Pistole from FBI and Mr. Allen from the DHS Office of Intelligence. Ms. Graham mentioned the structural changes to the IC and was questioned regarding information sharing and DNI authorities.

[143] Ibid., 23. Senator Dianne Feinstein specifically questioned information sharing down to the local law enforcement level.

[144] Senate Select Committee on Intelligence, "Sen. Dianne Feinstein and Rep. Mike Rogers Hold a Joint Hearing on the State of Intelligence Reform," Hearing before the Select Committee on Intelligence of the United States Senate held on September 13, 2011. <http://congressional.proquest.com.proxy3.library.jhu.edu/congressional/docview/t65.d0.09130003.s66?accountid=11752> (accessed June 24, 2013). It should be noted, counterterrorism remained at the forefront of this debate, but several hearing participants addressed cyber operations.

[145] *Reform of the United States Intelligence Community* S. Hrg 108-835, 85.

between terrorists and a specific country.[146] Both statements have strong parallels to cyber domain considerations, but went unaddressed in open hearing dialogue. SSCI Chairman Pat Roberts (R-Kansas) stated, "Distinctions between the domestic, foreign and defense intelligence just do not exist as of today's world."[147] Although, the Chairman and Vice Chairman recognized the changing intelligence landscape, neither saw fit to address the cyber domain in this context.

Senator Richard Durbin (D-Illinois) was the only SSCI member to address the interplay of national security and privacy early in the reform process when he questioned the presidentially created civil liberties board in the Department of Justice.[148] Senator Chuck Hagel (R-Nebraska) acknowledged there could be other threat areas beyond terrorism, which should be considered during the intelligence reform process, but noted weapons of mass destruction and narcotics in lieu of the cyber domain.[149] In 2007 when the committee devoted open hearing time to the reform process in DHS and FBI there was no investigation into cyber domain issues.[150]

However, in 2011 during a joint hearing with the HPSCI, ranking member C.A. "Dutch" Ruppersberger (D-Maryland) addressed cyber attack and security on the Korean Peninsula. In the same hearing SSCI Vice Chairman Saxby Chambliss highlighted his concerns surrounding the possibility FISA and USA PATRIOT Act sunset provisions might expire.[151] Overall, the SSCI was unable to look beyond the threat of terrorism during the intelligence reform process and failed to adequately take account of cyber

---

[146] Ibid., 87.
[147] Ibid., 130.
[148] *Reform of the United States Intelligence Community* S. Hrg 108-835, 121.
[149] Ibid., 118.
[150] *Intelligence Reform* S. Hrg 110-839, 77-106.
[151] "Sen. Dianne Feinstein and Rep. Mike Rogers Hold a Joint Hearing on the State of Intelligence Reform," 9 & 30.

domain issues. There were few cyber oversight examples available to analyze during the intelligence reform process. During the first decade of the 21st century; the cyber domain was not an integral consideration as the U.S. looked to restructure the IC to meet emerging threats. The SSCI used other venues to consider cyber domain operations and activities, but intelligence reform should have considered the cyber threat.

The USA PATRIOT Act. Three open hearings conducted by the SSCI in 2005 and dedicated solely to reviewing the USA PATRIOT Act, offer a better foundation than intelligence reform for evaluating committee cyber oversight. SSCI engagement during open hearings offered useful examples of domestic intelligence oversight in the cyber domain. By 2005, the SSCI was completing its second classified audit of procedures and practices for the use of FISA.[152] Senator Bond and Snowe's (R-Maine) involvement in writing USA PATRIOT Act Section 213 displayed legislative activism outside open hearings.[153] During the open hearings in April 2005, SSCI Chairman Roberts delved into the utility of administrative subpoenas in national security investigations. Vice Chairman Rockefeller explored the possibility of Security and Freedom Enhancement (SAFE) Act passage and its effect on wiretaps.[154]

These examples of legislative activism were followed shortly thereafter in May 2005, with Chairman Roberts proclaiming the need to explore legislative proposals for

---

[152] Senate Select Committee on Intelligence, *USA Patriot Act* S. Hrg 109-341 (Washington: U.S. Government Printing Office, 2005), 2.

[153] Ibid., 68-69. USA PATRIOT Act Section 213 relates to reasonable delayed notification of searches (with court approval) in terrorism cases. The Ninth Circuit Court originally set the notification precedent at 7 days with respect to criminal investigations, but notification delay debates continue in national security investigations

[154] Ibid., 88. SSCI member Senator Jon Corzine was a co-sponsor on the SAFE Act (S. 737) in April 2005 as another source of attempted strategic guidance to the IC on domestic intelligence collection. A key provision of the SAFE Act was to eliminate the combination of John Doe wiretaps and unidentified location (roving) wiretaps.

the PATRIOT Act mark up process.[155] During this open hearing the public was also privy to examples of IC strategic guidance alongside legislative activism. Senator Feinstein proposed two limitations be added to PATRIOT Act Section 213 if administrative subpoena power was to be granted to the DOJ.[156] Vice Chairman Rockefeller argued sunset provisions were a useful tool for examination based off arguments made by witnesses from the Open Society Institute and the Center for Democracy and Technology.[157] However, the inability of committee members to agree on the constitution of the word 'content' in legislative proposals highlighted a significant cyber oversight challenge in providing strategic guidance to the IC.[158] New technologies blurred the lines of information protected by privacy laws.

The SSCI demonstrated its ability to provide oversight through public advocacy and constitutional adherence during the USA PATRIOT Act review process. Witnesses from both sides of the ideological spectrum criticized and praised the act. SSCI committee members engaged in considerable debate regarding possible 4th Amendment violations contained in the PATRIOT Act.[[159]][[160]] Senator Carl Levin (D-Michigan) inquired about an ascertainment requirement similar to the criminal code, which preceded electronic surveillance in national security investigations.[161] Senator Bond inquired as to the consequences for federal agencies that operated beyond the law's limitations.[162]

---

[155] Ibid., 153.
[156] Ibid., 178-179. Senator Feinstein suggested administrative subpoenas be required to have Assistant U.S. Attorney authorization and an emergency requirement where other mechanism were unavailable.
[157] Ibid., 210-221.
[158] Ibid., 80.
[159] Ibid., 60, 72-73, 81-82.
[160] In 1976, U.S. v. Miller the U.S. Supreme Court determined no 4th Amendment Privacy interests pertained to records held in third party hands.
[161] Ibid., 110.
[162] Ibid., 175.

Senators Barbara Mikulski (D-Maryland) and Snowe both drew discussions towards the American citizenry in an attempt to clearly delineate which federal agencies had the power to collect on American citizens and how to best inform the public regarding the application of the USA PATRIOT Act.[163] The depth of debate and scope of questioning during the USA PATRIOT Act related open hearings satisfied the SSCI's public advocacy and constitutional adherence oversight responsibilities.

FISA and Other Inquiries. In 2007 and 2008 the SSCI held a series of hearings that broadly addressed different aspects of intelligence oversight. Several of these hearings provided useful evidence regarding SSCI oversight in the cyber domain. During the May 2007 open hearing regarding the modernization of FISA, SSCI members consistently explored the constitutional adherence of proposed changes to the FISA legislation. SSCI Chairman Rockefeller opened the question and answer session by inquiring about existing protections for incidental collection of U.S. person's communications.[164] Vice Chairman Bond reviewed proposed changes to the definition of a "foreign power" and adherence to the U.S. Constitution's 4th Amendment.[165]

Senators Feinstein and Whitehouse also explored legal issues regarding the President's ability to side step FISA. This argument stemmed from controversy over the TSP, which was authorized by President Bush using Article II powers and not divulged to SSCI members for five years.[166] Senator Snowe engaged in the constitutional adherence debate surrounding FISA modernization and asked DNI McConnell whether the proposed

---

[163] Ibid., 111 & 114.
[164] Senate Select Committee on Intelligence, *Modernization of the Foreign Intelligence Surveillance Act* S. Hrg 110-399 (Washington: U.S. Government Printing Office, 2007), 46.
[165] Ibid., 48.
[166] Ibid., 55-57. Senator Feingold addressed the President's use of Article II authorities in relation to the Terrorist Surveillance Program during both the Modernization of FISA hearing on page 52 and the Congressional Oversight of Intelligence hearing from page 39-40.

legislation would create loopholes that made judicial warrants for electronic surveillance the exception, not the rule.[167]

The SSCI met some of its other oversight responsibilities during these hearings as well. During the FISA modernization debate both Chairman Rockefeller and Vice Chairman Bond identified key attributes of FISA in need of legislative change.[168] Senator Wyden also identified broader privacy concerns he believed worthy of open debate.[169] In the 2008 review of DNI statutory authorities Senator Warner stressed the need for public awareness of the effect on tactical operations without FISA reform legislation.[170] During the debate over Congressional oversight of intelligence and its effectiveness, SSCI members spent considerable time lamenting powers the committee lacked.[171] As a witness before the committee, Dr. Zegart highlighted the fragmentation of IC reporting processes to a multitude of committees, for example the Judiciary and

---

[167] Ibid., 59.

[168] Ibid., pg. 2-4. Chairman Rockefeller proposed three possible changes to FISA. First, the AG should be required to have a court warrant to wiretap in the U.S. when a U.S. person is reasonably believed to be involved. Second, the AG needs to have a FISA court order based on probable cause before he/she has the authority to compel third party assistance. Finally, the Chairman wanted to ensure there was no part of the FISA amendments that would allow the President to resume warrantless wiretapping. Vice Chairman Bond proposed making "electronic surveillance" technology neutral. He wanted to update the term "content" to make it consistent with the FISA pen register and wanted to streamline the FISA application and order process. Vice Chairman Bond's recommendations were congruent with those changes proposed by IC officials.

[169] Ibid., 50-51. Senator Wyden engaged DNI McConnell regarding how the FISA changes would impact the privacy of Americans. He expressed concerns about the proposed changes based on precedents he felt were set during the administration's use of National Security Letters. Wyden also suggested the proposed legislation would grant immunity to those who supported the warrantless wiretapping under the Terrorist Surveillance Program.

[170] Senate Select Committee on Intelligence, *Statutory Authorities of the Director of National Intelligence* S. Hrg 110-837 (Washington: U.S. Government Printing Office, 2008), 24. During the debated regarding DNI statutory authorities SSCI members and IC officials debated the impact of the expiring Protect America Act. IC officials believed FISA amendments were required independent of the expiration of the Protect America Act. SSCI Chairman Rockefeller suggested the Whitehouse wanted to force the Senate to act on FISA amendments by refusing to sign an extension to the Protect America Act. DNI McConnell believed FISA amendments were required to provide liability protection to the private sector that cooperated with the IC.

[171] Senate Select Committee on Intelligence, *Congressional Oversight of Intelligence Activities* S. Hrg 110-794 (Washington: U.S. Government Printing Office, 2007), 3-40.

Homeland Security committees.[172] The reduced significance of geographical boundaries associated with the cyber domain increases the importance of Dr. Zegart's point. However, during open hearings of congressional oversight effectiveness the committee members did not address cyber domain oversight. SSCI members debated structural and external oversight obstacles vice internal oversight issues or topics relevant to the cyber domain such as divergent reporting streams.

The debate over Attorney General guidelines for national security investigations contained cyber domain oversight rhetoric. However, the broader debate centered around use of criminal investigative techniques for national security investigations. The constitutional adherence oversight principle was most often employed during this process. Senator Whitehouse discussed with FBI General Counsel Ms. Valerie Caproni the pen register and trap and trace use.[173] As a witness before the committee, the Assistant Attorney General for the Department of Justice discussed the role of FISA in domestic FBI operations and its effectiveness as a tool for oversight.[174]

SSCI inquiries into FISA modernization and other oversight related topics were substantial during targeted hearings in the last ten years. The committee asserted itself into the debate and actively engaged witnesses to explore issues of constitutional adherence within legislation. The SSCI provided a platform for public discourse regarding sensitive topics bordering on privacy infringement. The SSCI was not successful in resolving the debate surrounding domestic cyber domain activities through legislative activism or providing the IC clear guidance on conducting operations in the

[172] Ibid., 43.
[173] Senate Select Committee on Intelligence, *Attorney General Guidelines for FBI Criminal Investigations, National Security Investigations, and the Collection of Foreign Intelligence* S. Hrg 110-846 (Washington: U.S. Government Printing Office, 2008), 23.
[174] Ibid., 6.

cyber domain. Members did not utilize open hearings to untangle the web of foreign cyber threats and domestic cyber collection. This shortfall was consistent with similar shortcomings in the annual threat hearings reviewed.

RESEARCH FINDINGS

Three strengths and three weaknesses were identifiable after reviewing ten years of open hearings related to SSCI cyber oversight.

Cyber Oversight Strengths. The SSCI approached its oversight responsibilities in the cyber domain with a bipartisan spirit. Hearing dialogue between committee members consistently demonstrated a willingness to work in a bipartisan fashion when dealing with cyber related issues. This characteristic reinforces the historical narrative on the SSCI's spirit of bipartisanship. Although general consensus over the last two decades is the SSCI has grown more partisan; a review of cyber domain oversight contradicts this sentiment. In open hearings devoted to the exercise of oversight and not voting on legislative actions the atmosphere was generally dedicated towards informed debate. This conclusion suggests more nuanced study of SSCI partisanship is warranted.

SSCI cyber oversight in the last ten years also contrasts sharply with Senate IC oversight in the 1950s and 1960s. 1950s and 1960s IC oversight significantly influenced the major changes to oversight in the 1970s. In contrast, committee oversight in the cyber domain has existed for the last ten years, although at times misguided. There is strong evidence indicating the SSCI was not 'asleep at the wheel' regarding privacy issues and IC domestic surveillance operations. During the IC reform process after 9/11 the SSCI continuously engaged the administration, the IC, and outside experts regarding issues of constitutionality.

Finally, the SSCI was successful in addressing a multitude of technical and complex intelligence issues as the work bordered on classified information. Committee members generally offered thoughtful and insightful questions into cyber domain operations despite the extreme sensitivity associated with technical collection and analysis. This helped the SSCI to successfully accomplish most of its public advocacy responsibilities in cyber domain oversight.

Cyber Oversight Weaknesses. First, the SSCI approached domestic cyber domain oversight independent of foreign cyber oversight. Electronic surveillance for terrorism prevention requires engagement with the private sector, but was oft maligned by legislators fearful of privacy intrusions. However, the same engagement with the private sector was lauded when it was related to threats of cyber attack from foreign adversaries. Vague and conflicting strategic guidance to the IC regarding its cyber operations was the result. The SSCI must address foreign and domestic cyber domain operations simultaneously.

Building upon the first oversight weakness, the SSCI over the last ten years heavily focused on the threat of terrorism, while a clearly defined cyber policy was slow to develop. This issue likely transcends the SSCI and is applicable to Congress writ large, but was noticeable in the reviewed open hearing dialogue. The result of short fuse legislative activism regarding cyber domain operations reinforced the false distinction between domestic and foreign cyber oversight and justified the use of emerging technologies before oversight bodies were prepared with appropriate legislation.

Third, the terrorism focus in the last ten years swayed the debate regarding cyber domain operations far more towards domestic issues than to foreign issues. Threats to

national security were more diverse than terrorism, however cyber domain oversight remained tightly tied to terrorism prevention. Electronic surveillance targeting terrorists engendered debate regarding privacy invasions, while debate regarding a cyber attack's placement on the warfare spectrum remained underdeveloped. The IC has not received clear legislative and strategic guidance from the SSCI that bridges domestic and foreign cyber issues.

RECOMMENDATIONS

A thoughtful and well-defined bipartisan legislative proposal from SSCI members would begin to address cyber oversight shortfalls. This proposal needs to challenge the U.S. government's conceptual ideas regarding cyber domain operations. Terrorism can no longer be the only impetus for oversight in the cyber domain. The legislation surrounding IC collection in the cyber domain must pertain to all manner of threats, especially those emanating within the cyber domain itself. This is not to suggest all threats are created equal, therefore it is expected IC cyber domain legislation would contain caveats for threats, such as terrorism or weapons of mass destruction. However, a legislative proposal from SSCI members must build upon past statutes to further technological and geographically neutral legislation for IC cyber operations and provide enduring strategic guidance.

A bipartisan legislative proposal must also include a consensus opinion regarding the IC's freedom to operate in the cyber domain. Using an analogy from military aviation, the Air Force supplies its pilots a list of authorized tactics, techniques, and procedures (TTPs) while all other maneuvers are prohibited. In contrast, the Navy supplies its pilots a list of unauthorized TTPs, while all other maneuvers are acceptable.

The SSCI must provide one of these forms of strategic guidance to IC cyber domain activities. The Internet is largely unregulated space, which distinguishes it from many other facets of society. However, the SSCI must consider the strength of IC institutional prohibitions on privacy intrusions before it adopts the Navy's 'trusted pilot' approach to cyber operations.

Finally, the SSCI's legislative proposal should recommend the creation of a National Cyber Operations Center (NCOC) within the Office of the Director of National Intelligence. This office should have similar responsibilities to the National Counterterrorism Center and the Nation Counter-proliferation Center. It could serve to coordinate cyber operations across IC partners. The NCOC would not conduct cyber operations since NSA and U.S. Cyber Command already contain that mission, but NCOC could ensure standards for operational planning are met across the IC. Finally, the NCOC Office of General Council might be the most important component of the new division, as it would seek to bridge legal gaps in IC cyber operations.

CONCLUSION

This review of SSCI oversight in the cyber domain adds nuance to a blanket assumption of dysfunctional oversight. There is a strong argument that the SSCI successfully accomplished two of its oversight responsibilities --constitutional adherence and public advocacy--. However, it failed to actively propose useful legislation that provided clear strategic guidance to the IC. Clear strategic guidance for the IC in its cyber domain activities is essential. The role of the Internet and telecommunications in the lives of Americans grows continually. The diversity of threats beyond terrorism grows as well, and the IC can utilize technological superiority to address these threats. Threats existing

solely in the cyber realm require well-defined legislation to enable the IC to respond accordingly. The development of legislation requires the SSCI to address foreign cyber adversaries alongside domestic cyber operations. It is no longer acceptable to address domestic cyber operations in the context of terrorism and foreign cyber operations in the context of military operations. American national security in the 21st century will be dependent upon the government's ability to reconcile emerging foreign cyber threats with domestic cyber operations. However, SSCI oversight of the cyber domain will only contribute to national security if it can fulfill all four effective oversight principles and strengthen the public trust of the IC and oversight institutions.

CHAPTER THREE: 'IF ANGELS WERE TO GOVERN MEN'

In Federalist 51, James Madison stated, "[i]f men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."[175] The U.S. possesses the world's most advanced intelligence collection apparatus, but the IC requires enormous secrecy to protect the sources and methods it employs as it collects the information required to meet the state's intelligence needs. The U.S. government has granted considerable authority to the IC to accomplish its important mission. With that grant of authority comes the responsibility for both effective internal and external oversight. This external oversight is a shared role executed by the Executive and Legislative Branches. In a democratic society, determinations as to the effectiveness of that oversight are always subject to scrutiny and judgment by the citizenry. This public judgment is played out in the political process: one needs only to pick up a daily newspaper and follow the public outcry over the recent revelations of the scope of NSA data collection activities.

The American public must trust IC overseers, and understand their significance and their role. A dearth of research exists explicitly examining public perceptions of intelligence oversight. This chapter aims to offer unique public opinion analysis based on an original survey. Gathering public perceptions of the significance, structure, and effectiveness of IC oversight helps inform political decision-makers of public expectations. These perceptions offer researchers and legislators the opportunity to

[175] James Madison, "The Federalist No. 51." Web. <http://www.constitution.org/fed/federa51.htm>.

expand theories of intelligence oversight and adapt political behavior. Most importantly, an informed populace with a better understanding of the IC and greater confidence in IC oversight creates a bond of trust between a critical government institution and the American public it strives to defend.

PUBLIC OPINION AND THE INTELLIGENCE COMMUNITY

According to Theodore Lowi, "[t]he basic idea behind democracy holds that the sum of many millions of votes produces a better outcome than the decision of a small number of people"[176] American's generally hold common ideas and principles regarding government and society. The aggregation of these commonly held beliefs gives legislators an understanding of the public's opinion and in a representative democracy such as the U.S.; it serves to shape legislators' decisions.[177] They are most often responsive to their constituents because they must compete for reelection.[178] In the case of intelligence policy and oversight, public opinions are often shaped by an incomplete understanding of the IC and its oversight institutions.[179]

Americans have strong beliefs in the Constitution of the United States, and the concepts of individual liberty and equal rights under the law. In general, these beliefs are embedded in the fabric of the American people. However in specific policy areas the American public can be divided between supporting government action or inaction. Lowi points out, "[p]ublic opinion…should not be thought of as a single-minded view or

---

[176] Theodore J. Lowi, *In American Government: Power and Purpose*, 11th ed (New York: W.W. Norton, 2010), 363. This concept is derived from Jury Theorem by Marquis de Condorcet.
[177] Ibid., 360-365. Lowi suggests that Congress is generally more attuned to public opinion than the President because legislators must worry more about ignoring their constituents' concerns.
[178] Lawrence R. Jacobs, Eric D. Lawrence, Robert Y. Shapiro, and Steven S. Smith, "Congressional Leadership of Public Opinion," *Political Science Quarterly* 113 no.1 (1998): 22.
[179] In Congress the institutions with primary responsibility for IC oversight are the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).

consensus on a given matter, but as a range of options."[180] American citizens form their opinions through individual beliefs and experiences.[181] The ability to express opinions freely in myriad ways on issues such as intelligence oversight gives overseers the opportunity to be responsive to public opinion shifts.

Scholarly literature often suggests the degree to which public opinion influences policy is associated with the salience of an issue. However, even in the face of interest groups, economic elites, and political parties, public opinion can influence policy.[[182]][[183]] There are also strong arguments areas with lower salience levels such as foreign policy and defense still maintain high levels of policy responsiveness to public opinion. Paul Burstein offers,

> [t]he data on foreign and domestic policy provide no support for the hypothesis [that domestic issues will generate greater government responsiveness to public opinion]. Of the ten coefficients gauging the relationship between opinion and defense policy (nine on expenditures, one on the Vietnam war), all are statistically significant; on defense, government is more responsive to the public than on other policies, not less.[184]

---

[180] Lowi, *In American Government: Power and Purpose*, 367.

[181] Ibid., 370-381. According to Lowi the three influencers of opinion are 1) perceptions of how government actions will affect individuals, 2) the political socialization and the influence of family, education and social groups affect opinions and, 3) opinions are driven by political ideology and the expected role of the state. Once opinions are formed they are expressed through voting, campaign contributions, lobbying, letters, blogs, political activism and other ways.

[182] Benjamin I. Page and Robert Y. Shapiro, "Effects of Public Opinion on Policy," *The American Political Science Review* 77 no.1 (1983): 177-182. In examining 231 cases, Page and Shapiro found policy was congruent with public opinion within one year in 66 percent of cases. In addition, they found the same level of congruence on foreign and domestic policy issues and also that the salience of the issue did not appear to impact the level of congruence.

[183] Paul Burstein, "The Impact of Public Opinion on Public Policy: A Review and an Agenda," *Political Research Quarterly* 56 no.1 (2003): 29. The degree of impact is the primary source of debate regarding the effect of public opinion on policy. Burstein finds that "public opinion influences policy most of the time, often strongly. Responsiveness appears to increase with salience, and public opinion matters even in the face of activities by interest organizations, political parties, and political and economic elites. Claims that responsiveness is changing over time or varies across issues rest on very little evidence" (Burstein, pg. 29).

[184] Ibid., 36.

Buttressing Burstein's conclusions, Hartley and Russert find that public opinion has a significant effect on military spending over time.[185] These findings underscore the importance of public opinion on issues with less salience, such as intelligence oversight. As public opinion shifts regarding the activities of the IC and as time passes from a coalescing event such as the terrorist attacks of 9/11, policymakers must be aware of opinion shifts in order to be responsive to public expectations.

Although most of the scholarly literature suggests public opinion shapes political behavior, intelligence policy is influenced by unique factors that complicate the situation. In the case of the IC, few constituency groups are directly affected by intelligence policy and few legislators and members of the public possess an intimate knowledge of the issues. The secrecy surrounding IC activities does not engender an informed public. These issues integrate well with research conducted by Jacobs, Lawrence, Shapiro, and Smith, who propose that congressional leadership is more responsive to public opinion than rank and file members.[186] Legislators' ability to shape public opinion frees them from the obligation to be responsive to it. However, without an accurate understanding of public opinion on intelligence oversight, legislators are operating blindly and can set the stage for severe public backlash against controversial policies.

---

[185] Thomas Hartley and Bruce Russert, "Public Opinion and the Common Defense: Who Governs Military Spending in the United States?," *The American Political Science Review* 86 no.4 (1992): 911. Their evidence indicates, "increases in the percentage of the public that believes that the government is spending too little on the military result in increases in military spending ($b = .261$, $p < .05$). The statistical significance level for this independent variable is impressive, considering that the indicator is the average of values taken from different survey houses" (pg. 910).

[186] Jacobs, Lawrence, Shapiro, and Smith, "Congressional Leadership of Public Opinion," 24-41. The authors concluded that "[t]he shaping of public opinion by leaders may offer the key to solving the puzzle of public opinion's muted impact on individual legislators, but its significant influence on the collective behavior of Congress…[because] leaders have the capacity under particular circumstances to bring the public around to adopting their preferred policies" (pg. 41). In their research the 1993-1994 health care reform debate was assessed because of the unique ability Republican lawmakers had to reject polling indicators and shape public opinion.

No review of public opinion could be complete without addressing public perceptions of Congress. Public opinions of intelligence oversight and policy are wrapped within opinions of Congress writ large. According to the Pew Research Center, in April 2010, 65 percent of Americans viewed Congress unfavorably and suggested Congress was having a negative impact on the direction of the country.[187] The public's discontent with Congress was most apparent in the 52 percent of Americans who believed the overall political system worked fine but that the "problem" was with members of Congress.[188] By January 2013, that number had grown to 56 percent.[189] Pew research in 2013 also indicated a majority of Americans believed the federal government was a threat to their personal rights and freedoms, while 68 percent had unfavorable views of Congress.[190] Although a simplistic analysis of these statistics could lead to the conclusion that the opinions regarding congressional oversight of the IC were similarly negative it is important to gather granularity on the public's views of intelligence oversight. There is a unique relationship between Americans and the IC and a survey of the public's opinion on this issue is the first step to assessing effects over time and setting a foundation where policymakers legislate informed by public opinion.

U.S. CONGRESSIONAL OVERSIGHT OF INTELLIGENCE

---

[187] Pew Research Center, *Distrust, Discontent, Anger and Partisan Rancor: The People and Their Government* (Washington, DC: Pew Research Center for the People and the Press, 2010), 43 & 52. Also noteworthy, the Central Intelligence Agency had a 51 percent favorability rating in 1997 and a 52 percent favorability rating in 2010. According to the Pew Research Center federal agencies and institutions were viewed far more favorably than Congress.

[188] Ibid., 6. In contrast only 38 percent of Americans indicated the political system was broken and members of Congress had good intentions. However, 79 percent of Americans did agree the government was facing more complex problems than it had in the past, a sentiment worth noting in consideration of the complexity surrounding national security threats and the IC.

[189] Pew Research Center, *Majority Says the Federal Government Threatens Their Personal Rights: Views of Congress* (Washington, DC: Pew Research Center for the People and the Press, 2013), 9.

[190] Ibid., 1-3.

Formal congressional oversight of intelligence activities in America was born out of IC abuses that came to light in the middle 1970s. Pre-1975, Congress exercised its intelligence oversight responsibilities informally, despite their defended existence in the U.S. Constitution's necessary and proper clause.[191] In other public policy areas Congress has long exercised its oversight responsibilities through formal institutions and processes, but for IC oversight between 1947 and 1975, oversight was an informal process.[[192]][[193]]

Publication of the "Family Jewels" in the New York Times became the impetus for the Church Committee, Pike Committee, and Rockefeller Commission.[194] All three investigative bodies concluded more formal oversight mechanisms were required for the IC. Therefore, to cure the ills plaguing the IC the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) were created to provide formal oversight. While the creation of these congressional committees institutionalized the intelligence oversight process, a multitude of challenges to effective oversight remained.[195]

Public perception is critical for the IC because it dictates whether legislators will have the political backing of their constituents to authorize and appropriate resources without significant public insight into how those funds are used. Mark Lowenthal

---

[191] U.S. Constitution, Article I, Paragraph 8, Section 8- "Congress shall have the Power…To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in Department or Officer thereof."
[192] Loch Johnson describes 1947 to 1975 as the Era of Trust between policymakers and the intelligence community.
[193] Mark Lowenthal notes that the U.S. is unique from other countries in the extensive oversight responsibilities for intelligence activities that are placed upon the legislative branch.
[194] The "Family Jewels" were uncovered by Seymour Hersh and identified CIA abuses that included a domestic mail opening program and assassination plots abroad. However, between the three investigative bodies the FBI's COINTEL program, Army intelligence programs and NSA programs were revealed to be operating far outside their legal bounds and often in violation of American civil liberties.
[195] For additional reading on the creation of the modern IC and congressional oversight of the IC see Frank Smist, *Congress Oversees the United States Intelligence Community 1947-1993*, Loch Johnson, *A Season of Inquiry: Congress and Intelligence*, and Mark Lowenthal's, *Intelligence: From Secrets to Policy, 5th ed.*

identifies one of the three key components to the relationship between Congress and the IC as the "public perception of intelligence and support for it."[196] This aspect to the relationship between Congress and the IC gives legislators good reason to provide effective oversight. However, there are well-established criticisms of congressional oversight of intelligence that offer the foundation for studying public opinion of intelligence oversight.

The most commonly studied issue related to congressional oversight is its effectiveness and the continuity of attention legislators provides the IC. Loch Johnson suggests Congress has fluctuated between a "police patrolling investigative" approach and a "reactive fire-fighting" approach to oversight.[197] He concludes that full engagement of congressional resources towards IC oversight only results when loud alarm bells are sounded and garner the attention of the American electorate.[[198]][[199]] Johnson's explanation of oversight extends beyond presidential administrations and crosses party lines. When alarm bells are sounded loud enough for a multitude of Americans to react, intelligence issue salience is driven up by the news media and forces a Congressional response.

---

[196] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. 5th ed (Washington DC: CQ Press, 2012), 46-47. The other two key components to the relationship between Congress and the IC are personal relationships and Congress' control of intelligence community funding.

[197] Loch Johnson, "Accountability and America's Secret Foreign Policy: Keeping a Legislative Eye on the Central Intelligence Agency," *Foreign Policy Analysis* 1 (2005): 102. The fire fighting and police patrolling approaches to oversight are derived from Aberbach's research into models of congressional oversight. Johnson breaks into four eras the relationship between Congress and the IC; Era of Trust (1947 to 1974), Era of Uneasy Partisanship (1975 to 1986), Era of Distrust (1986-1991), Era of Partisan Advocacy (1991 to 2001), and Era of Ambivalence (2001 to present).

[198] Ibid., 103.

[199] Amy Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (California: Hoover Institution Press, 2011), 3-5. The 9/11 Commission made special mention of intelligence oversight shortfalls and dysfunction. It prompted a debate for simplifying congressional oversight of intelligence, but resulted in little action for the next 6 years.

Another common theme in oversight dysfunction literature stems from intelligence overseers lacking incentives to provide effective oversight. Amy Zegart suggests legislators lack strong electoral incentives to focus on oversight as a result of demands on time and few constituents who vote based upon IC oversight decisions. The IC is a unique institution that requires attention and expertise to effectively oversee. Her scholarship suggests current congressional IC oversight structure is not capable of providing effective oversight.[200] The history and characteristics of IC oversight underscore the importance of gathering the public's opinion regarding intelligence oversight today.

RESEARCH METHODS AND SUMMARY STATISTICS

The purpose of this study was to gather public opinions regarding; 1) the significance; 2) structure; and 3) effectiveness of IC oversight by Congress. During November 2013, respondents were asked 18 intelligence oversight questions related to the three aforementioned categories. The survey was designed for a moderately informed respondent due to the complexity and narrowness of the topic. Despite the nuanced subject matter the study has significant value to researchers and legislators because it approached intelligence policy from a wholly unique angle then past research. Instead of gauging oft-collected public opinions on national security or defense spending, this study gathered opinions on how congress should manage its oversight responsibilities. It attempts to simultaneously address issues of government policy as well as underlying beliefs in the relationship between the IC, the oversight committees, and the public.

[200] Ibid., 36-39. Zegart's arguments are drawn from Rational Choice Theory and committee assignments that deliver the most significant political benefits drive political behavior. She also suggests "Congress will exercise less oversight in matters of national security than domestic policy" (pg. 41).

As a result, policymakers and congressional leaders have the opportunity to take stock of the public's opinion of intelligence oversight. This research serves as an avenue for participation and a mechanism for representation.[201] Although, congressional leaders lack large IC related constituencies as drivers of political behavior, those who are stewards of the IC have prestige and recognition to gain through effective oversight. This was a unique opportunity in modern history to study public opinion of IC oversight.[202] The salience of IC issues and its oversight was atypically high given recent leaks of classified information. The technical intelligence collection capabilities of the National Security Agency (NSA) and concerns of infringements upon American civil liberties engendered national level debate in the news media and at local coffee shops.[203]

No one electoral constituency has a monopoly on national security issues, therefore legislators overseeing the IC can approach oversight with statesmen-like attitudes focused beyond personal electoral incentives. This survey provides policymakers with a practical foothold for public opinions regarding the balance between civil liberties and national security. It conveys a different message to lawmakers because IC oversight does not have a direct daily impact on the lives of Americans, but is intertwined with American values and national security.[204] Lacking a direct daily effect

---

[201] Sydney Verba, "The Citizen as Respondent: Sample Surveys and American Democracy Presidential Address, American Political Science Association 1995," *The American Political Science Review* 90 no.1 (1996): 1-2. Verba argues that democracy implies equal consideration and responsiveness by policymakers to all citizens.

[202] Henry E. Brady, "Contributions of Survey Research to Political Science." *Political Science and Politics* 33 no.1 (2000): 47-57. Brady suggests, "creative uses of telescopes, microscopes, and sensors can take advantage of serendipitous naturally occurring events, [and] new survey designs can assess the causes and impacts of events such as debates, scandals, speeches, elections, coups, or revolutions that occur during the course of a survey project" (pg. 47).

[203] Glenn Greenwalk, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, (June 5, 2013). It was subsequently revealed the leaks emanated from former defense contractor Edward Snowden who fled the U.S. and sought asylum abroad.

[204] Verba, "The Citizen as Respondent," 2. This concept is derived from Verba's discussion regarding demographic groups most advantaged to influence government. In the case of IC oversight all

on the lives of Americans it is all the more important legislators have a clear understanding of public opinion before setting IC policy. The survey's contextual questions set forth the public's purpose and goal for congressional oversight of intelligence activities. They also help infer whether the public believes current oversight institutions are effective.

There were important considerations made when choosing to conduct a survey and designing survey questions. Non-probability sampling was used to improve the likelihood respondents were moderately engaged in national security issues and could offer informed opinions regarding IC oversight.[205] Using opportunistic and snowball sampling the survey was administered through electronic mail and the social networking site, Facebook.[206] It was made available to Johns Hopkins University, Advanced Governmental Studies students and staff, staff members of the Senate Select Committee on Intelligence, personal contacts of the researcher outside government, and members of the Department of Defense and IC. There was value in offering government officials the opportunity to respond to the survey questions anonymously because the nature of their career provides them unique insights into the workings of the IC and intelligence oversight. There was undoubtedly selection bias since staff members of the SSCI were permitted to take the survey, however their responses provided an anonymous "insiders" perspective on the IC oversight.

---

demographic groups are disadvantaged as a result of the secrecy and complexity of the community. In addition, Verba highlights national security issues as having low differential political activity levels because they are less impactful on the daily lives of Americans.

[205] Ibid,. 4. Verba suggests the advantage to using a survey in political science research is the ability to chase down individuals and ask them questions; there is no opportunity for quiescence in a survey.

[206] Balnaves, Mark, and Peter Caputi, *Introduction to Quantitative Research Methods: An Investigative Approach* (London: Sage Publications, 2001), 95.

All the survey questions were close-ended in order to gauge the respondent's values on issues they were unlikely to contemplate daily. The questions were randomly organized but addressed the three previously mentioned categories within IC oversight in order to successfully elicit perceptions of oversight.[207] Nominal variable questions and ratio variable questions in all three oversight categories offered respondents the opportunity to think about oversight from different angles. In order to address internal validity, specific questions intentionally allowed respondents to respond with *'no opinion'* or indicate the respondent *'lacked the background knowledge'* to answer. These options helped infer whether respondents believed IC oversight issues were sufficiently important to form an opinion during the survey.[208] Finally, 10 demographic related questions were included in the survey tease out portions of the sample for further analysis.

In order for a respondent's answers to be included in the final analysis, respondents were required to self describe as "moderately" or "often engaged in national security issues" or correctly answer two of the three factual national security related questions. These stipulations intentionally attempted to remove respondents who did not have the prerequisite background knowledge to participate in the study. The results offer a better understanding of the public's beliefs regarding oversight of the IC and offer lawmakers an opportunity to set policy that adequately represents the opinions of Americans. The survey received 117 respondents in November 2013, however 30 respondents were eliminated for failing to answer a majority of the survey questions and

[207] Pew Research Center for the People and the Press, *"Methodology,"* < http://www.people-press.org/methodology/> (accessed August 27, 2013).
[208] Brady, "Contributions of Survey Research to Political Science," 54. Brady highlights the value surveys possess in understanding policy relevance and participation.

2 other respondents were eliminated for failing to meet the standards for background knowledge. This left 84 respondents to analyze and draw conclusions on perceptions of IC oversight.

Table 1. National Security Survey Summary

Descriptors	Significant Percentages
Respondents < 41 years old	57.1%
Male Respondents	61.9%
Respondents w/ Government Affiliation	59.5%
Respondents Often Engaged in National Security Issues	68.7%
Moderate	50.0%
Conservative	29.8%
Liberal	15.5%
100% Correct Factual Responses	77.7%
No Trust of IC Coverage in the News Media	26.2%

Table 1 illuminates several important key features in the sample. A significant percentage of survey respondents were male, under the age of 41 and had some affiliation with the federal government. It is also noteworthy the sample included a larger percentage of individuals who viewed themselves as conservative vice liberal. These percentages are reminders that the sample is not representative of the entire U.S. population, but they aren't so large to discredit the external validity of the entire survey. The sample is undoubtedly a unique subset of the population, representative of individuals who often consider national security issues as a result of their occupations and can offer valuable IC oversight ideas to legislators and policymakers. However, the sample also includes individuals outside the government who maintain more liberal views regarding IC oversight, but also remains engaged in national security issues.

Several questions addressed self-perceptions to help draw conclusions about the relationship between the respondents and the issue of oversight. A large percentage of respondents perceived themselves as *often engaged on national security issues*, and a large percentage also answered all three factual oversight questions correctly. This suggests respondents were generally informed of national security issues and had previously given thought to the complex issues considered in the survey questions.

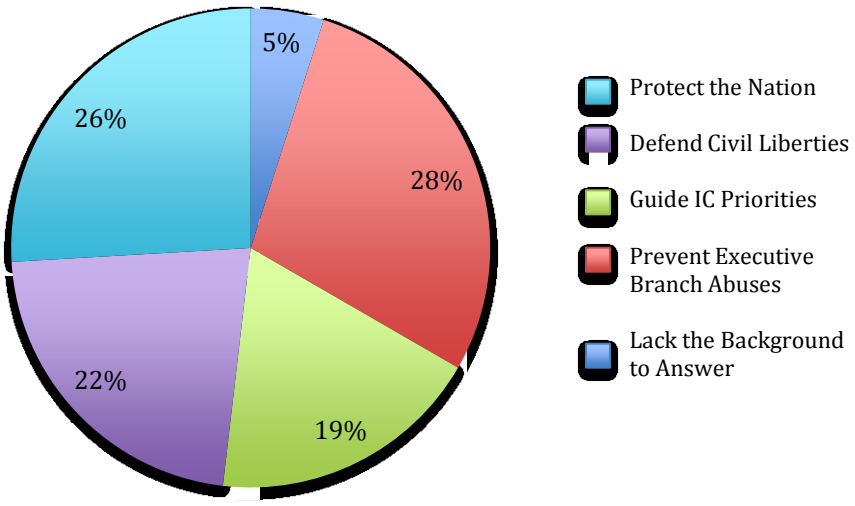
Table 2 offers several general conclusions the survey data from cumulative scale questions that contained degrees of diverging positions. The positive and negative spectrums in Table 2 present the opposing positions without consideration for the degree of a respondent's position. On cumulative scale oversight questions the data suggests respondents strongly believe in some degree of a hands-on approach to intelligence oversight. However, respondents were not as confident in a strong degree of effectiveness to the oversight currently provided. In addition, a majority believed the oversight committees hindered, to some degree, the ability of the IC to execute its duties.

Table 2. National Security Survey Overview

Perceptions on Congressional Oversight Effectiveness	Positive Spectrum	Negative Spectrum
Hands on versus Hands off approach to Oversight	79.5%	16.7%
Effective versus Ineffective Oversight	47.6%	36.6%
Committee Oversight Improves IC versus Hinders IC	30.5%	56.6%
Transparency versus Secrecy in Intelligence Oversight	36.3%	63.0%
Perception of Privacy versus Collection	20.2%	39.3%
Committees' Ability or Motivation to Protect Civil Liberties	72.3%	27.7%
Confidence that Oversight can Prevent IC Abuses	22.4%	42.6%
Trust in Information Provided by the Committees	32.1%	26.2%

Table 2 also illuminates several interesting leanings on the balance between civil liberties and national security. A majority leaned towards the need for secrecy in intelligence oversight and believed, to some degree, the government should be able to collect information about Americans. A greater number of respondents thought the intelligence oversight committees were unable to prevent IC abuses, but a strong majority believed the intelligence committees had the ability and/or motivation to protect American civil liberties.

Figure 6. Purpose of Congressional Oversight



The hands-on approach to oversight combined with need for secrecy, but a belief in an inability to prevent abuses suggests respondents held high expectations for congressional oversight and a strong belief in Congress' role in intelligence oversight. Figure 6 presents the wide distribution of respondents' ideas about the purpose of intelligence oversight by Congress. Overall, the strongest consensus supported preventing Executive Branch abuses, but defending civil liberties and protecting the U.S.

were within 10 percentage points. The purpose of the survey was to evaluate the effectiveness, significance, and structure of intelligence oversight by Congress. Building upon the summary statistics, analysis of the three oversight categories reveals clear indications that respondents believe in the importance of the intelligence committees, but hold concerns regarding its structure and effectiveness in certain areas.

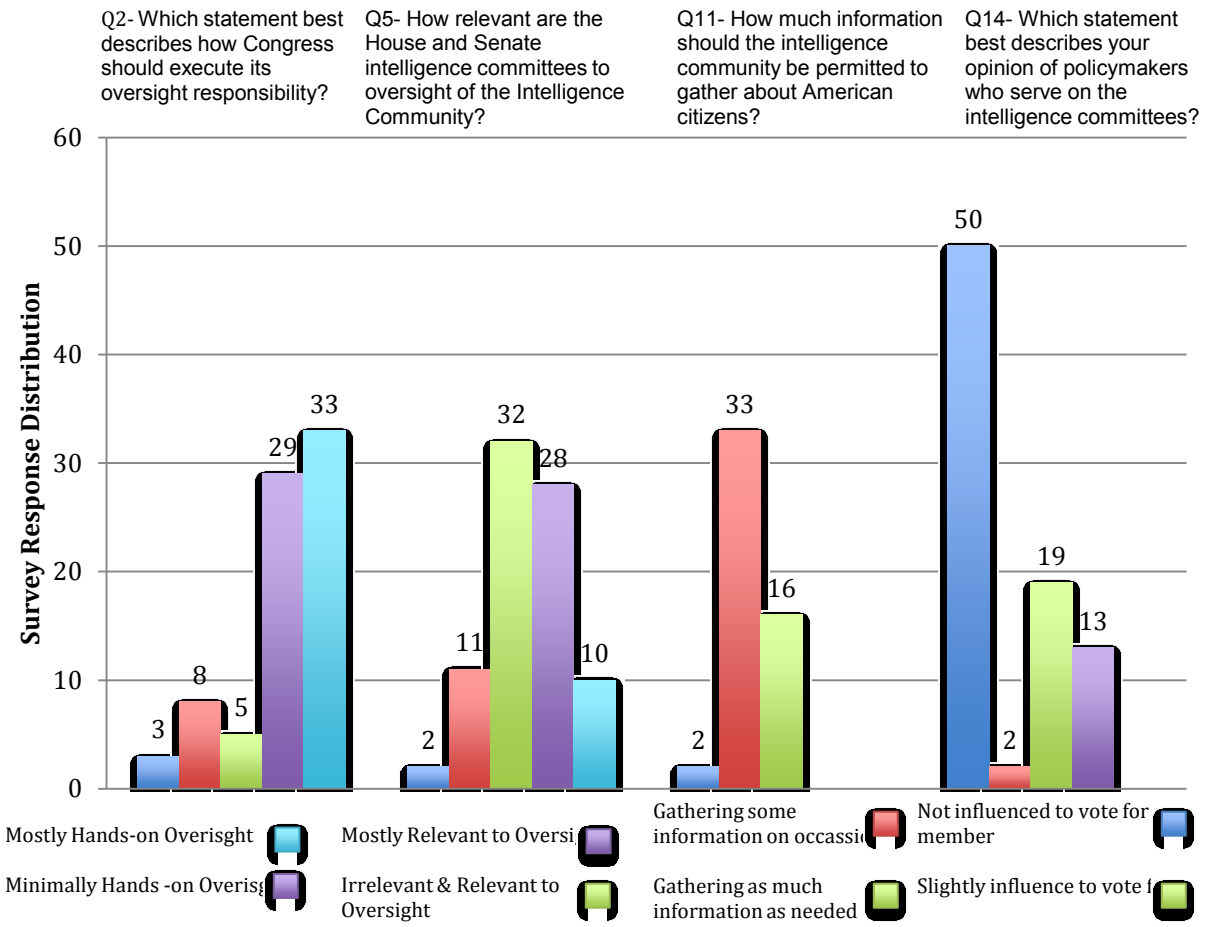
ANALYZING PERCEPTIONS OF OVERSIGHT

The Significance of Intelligence Oversight. There were five questions in the survey designed to assess perceptions of the significance or importance of intelligence oversight by Congress. Two differential scale questions identified perceptions of policymakers who serve on the intelligence community and suggested how congress should execute its oversight responsibility. Two cumulative scale questions evaluated the relevance of the intelligence committees and the leeway the IC should have to collect information on Americans. Finally, one nominal variable type question provided perceptions of the purpose for intelligence oversight.

The results of the survey suggest respondents supported a "hands-on" approach to intelligence oversight and a strong leaning towards at minimum, occasional IC collection of information on Americans. There was also a strong indication respondents believed the intelligence committees were relevant to intelligence oversight. All three of these indicators suggested respondents believed the intelligence committees were significant institutions. Figure 7 depicts these results, but also contains a negative measure of significance for the intelligence committees given the low likelihood that service on the committees would influence respondent vote choice. However, this negative indicator is

not too surprising given the traditional limited visibility of committee membership and

Figure 7. Intelligence Committee Significance



the lack of direct daily effect of intelligence oversight in respondents' lives.

Figure 6 depicts the diversity of opinions surrounding the primary function of intelligence oversight. There was a low plurality of respondents suggesting intelligence oversight existed to prevent executive branch abuses, but the relative equality among all options was another indicator intelligence oversight was significant to different respondents in different ways. Additionally, the measure permitting collection on Americans complements a "hands-on" approach to intelligence, suggesting respondents

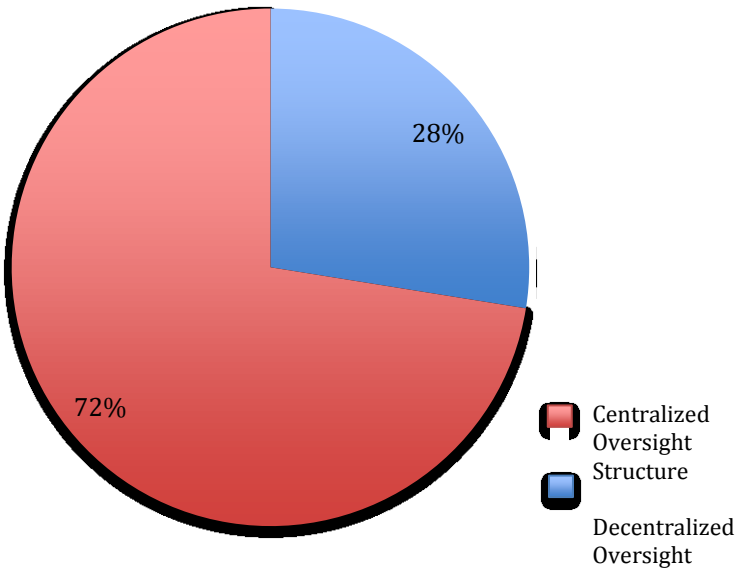
want active and investigative intelligence committees to prevent executive branch abuses. This supports the notion the intelligence committees remain relevant today and at least 40 percent of respondents indicated participation on one of the intelligence committees could have some influence on their vote choice. Lately, the intelligence committees have received intense public scrutiny, but over the last 35 years have had an important role in American government. The results of this category suggest intelligence oversight is significant in the minds of respondents and reinforces the continued importance of these institutions

The Structure of Intelligence Oversight. Five other questions within the survey gathered perceptions about the current structure of intelligence oversight. These questions were not designed to parse responsibility for intelligence oversight between one congressional committee or another. Instead, the questions examined elements influencing oversight structure such as secrecy or intelligence failures. Nominal variable type questions asked respondents for the causes of oversight failures and the nature of centralized oversight institutions. One cumulative scale type question explored perceptions of the proper balance between secrecy and transparency in intelligence oversight by Congress. The two final questions in this category addressed oversight committee responsibilities and the relative distribution of intelligence related information to members of Congress.

In this category, respondents overwhelmingly indicated a preference for a centralized structure within a few key institutions [Figure 8]. This suggests the existing oversight institutions are generally structured properly and perhaps in need of greater centralized control in oversight functions. Complementary to this, a plurality indicated intelligence oversight work should have more secrecy and less transparency [Figure 10].

Figure 8 indicates respondents believed oversight failures were most often the inability to understand or identify a problem, but not a failure to investigate or highlight a problem. This suggests respondents do not believe current oversight structures are complicit in abuses or suffer from significant "regulatory capture." Figure 11 ties these perceptions together; indicating a plurality leaned towards mild changes in the roles and responsibilities of congressional overseers. The results support centralized oversight in the hands of a few trusted congressional leaders with regular access to important information, along with the freedom to operate in secrecy. Most scholars would likely argue congressional oversight of the IC was in need of at least mild changes before this

Figure 8. Centralized Versus Decentralized Oversight



survey. However, the survey adds that if legislators could overcome internal obstacles to reform they would find favorable public responses.

Figure 9. Causes of Oversight Failures

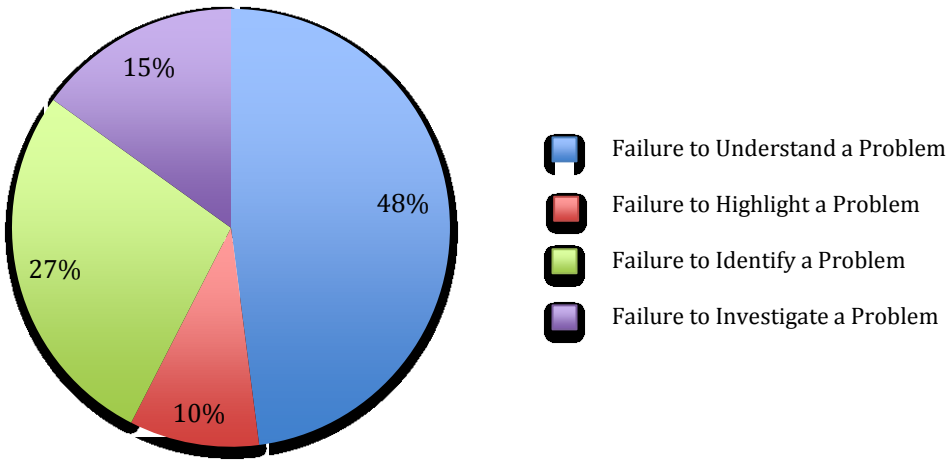


Figure 10. Transparency versus Secrecy in Oversight

Q7- On the scale below, identify the proper balance between transparency and secrecy in intelligence oversight?

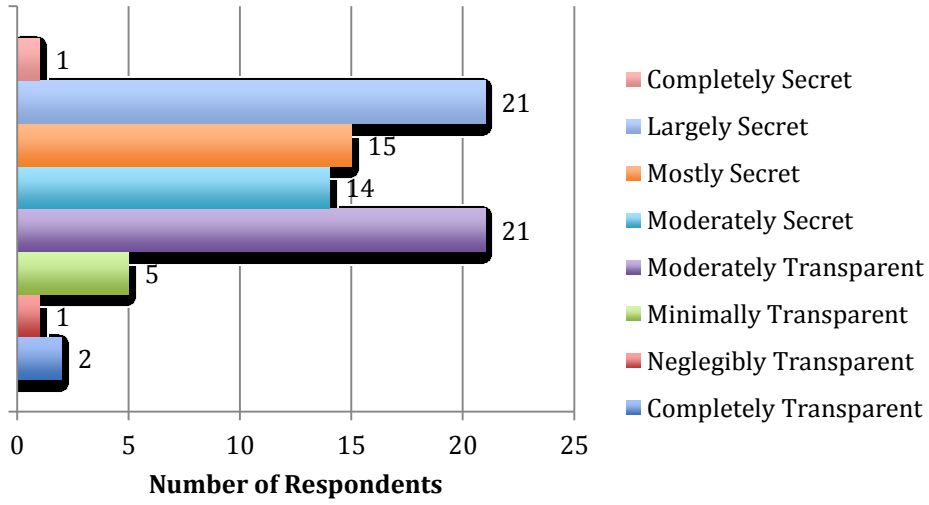
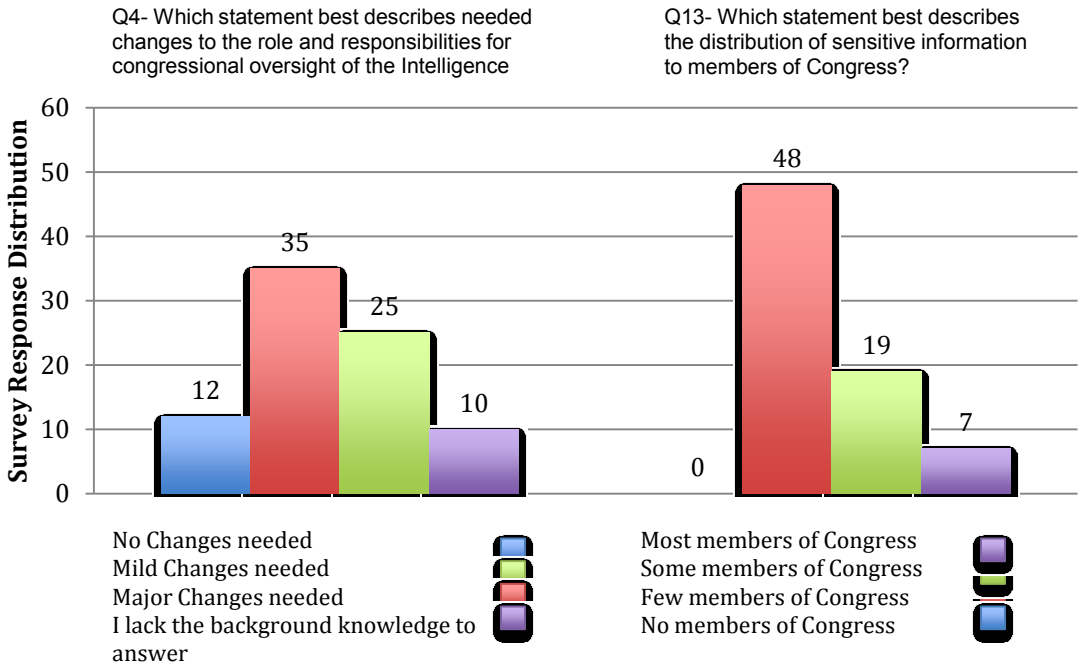


Figure 11. Structural Changes in Oversight



The Effectiveness of Intelligence Oversight. The largest category within the survey assessed the effectiveness of intelligence oversight by Congress. One nominal variable type question addressed the greatest obstacle to intelligence oversight. Three cumulative scale questions addressed committee effectiveness, the capability to prevent IC abuses, and respondent trust in the information provided by the intelligence committees. Four other differential scale questions extrapolated opinions on effectiveness through oversight influence on the IC, ability to protect civil liberties, and the effect of partisanship on intelligence oversight. These eight questions led to conclusions regarding respondent perceptions of oversight effectiveness.

Figure 12. Statements of Oversight Effectiveness

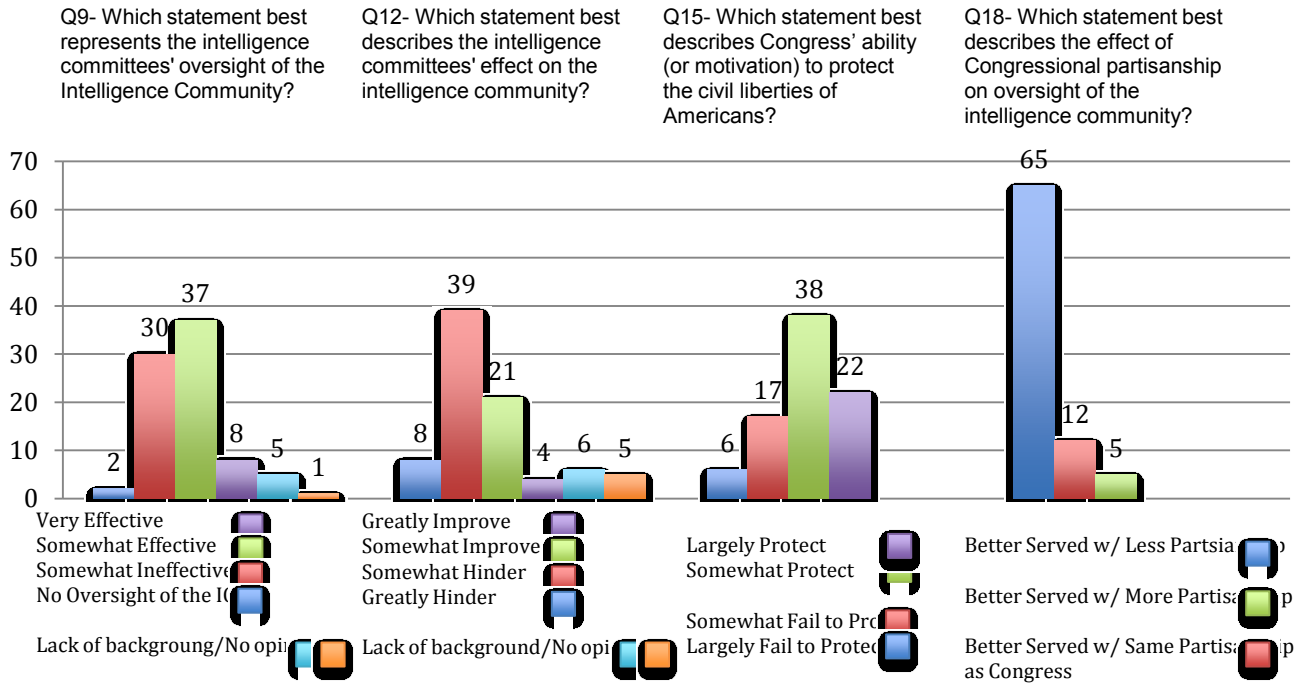


Figure 13. Obstacles to Effective Oversight

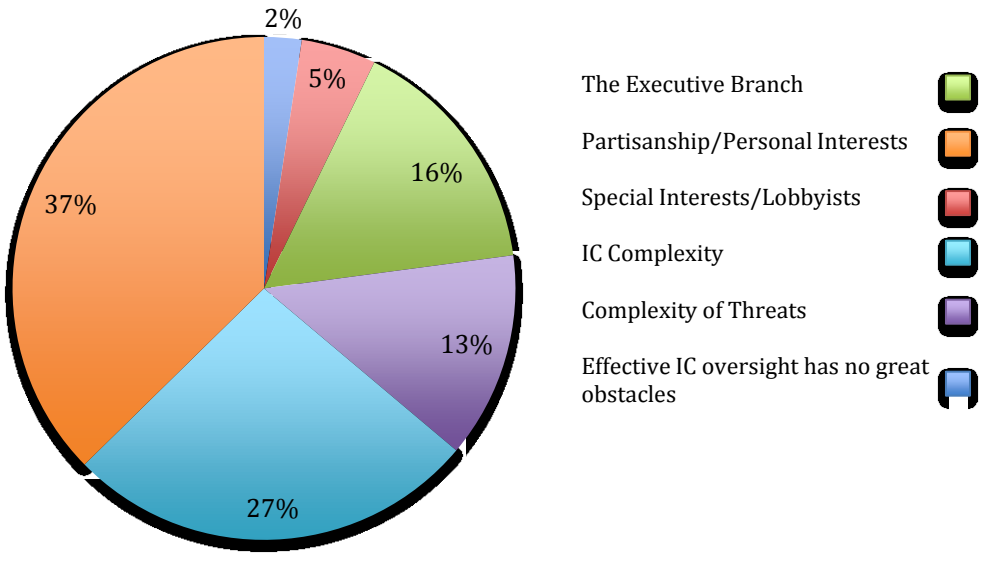


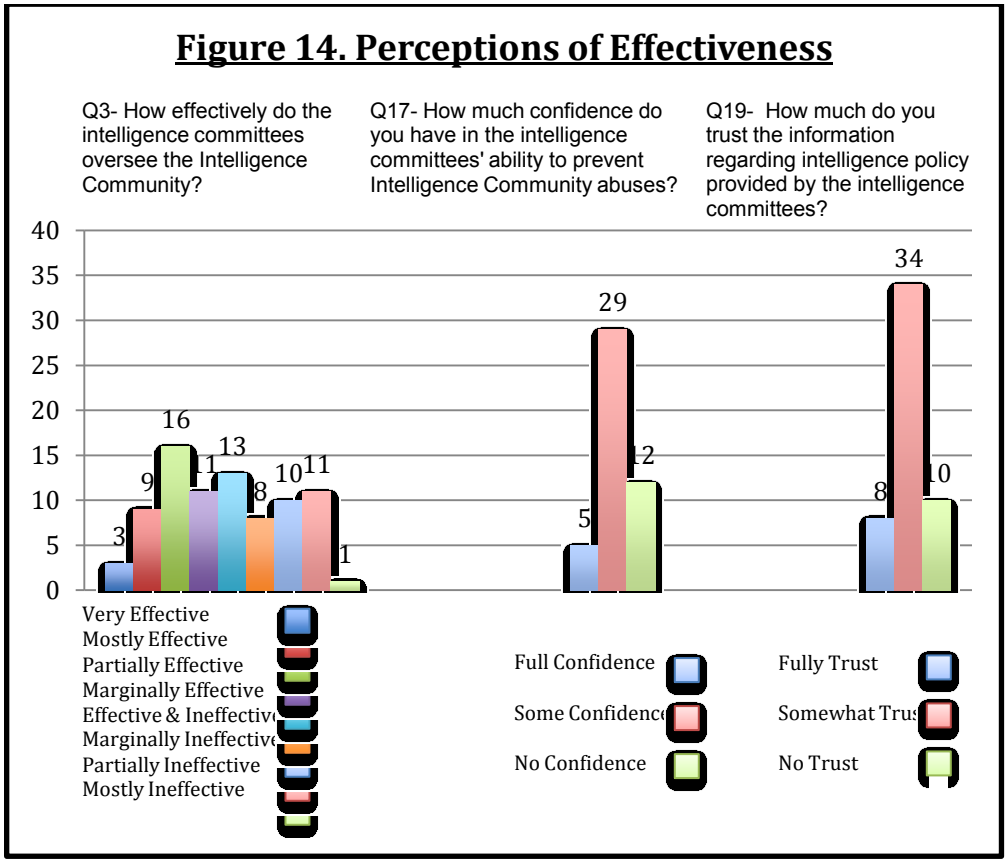
Figure 12 depicts all four differential scale questions and suggests respondents generally view the intelligence committees as somewhat effective in providing intelligence oversight. Two different positive measures of effectiveness were displayed by the 54 percent of respondents who perceived "effective" or "very effective" intelligence oversight by the intelligence committees and the 72 percent majority who believed the oversight committees were somewhat or largely capable/motivated to protect American civil liberties. However, a majority indicated partisanship inhibited oversight effectiveness and a plurality of respondents also indicated that intelligence oversight hindered the IC in its mission. These results suggest a nuanced belief in effectiveness among respondents.

Figure 13 built upon the nuance effectiveness concept by indicating respondents believed the greatest obstacle to effective oversight was partisan politics or increased partisanship. A plurality placed partisanship as the greatest obstacle to effective oversight above the executive branch, special interests, IC complexity and the complexity of threats. This measure appears congruent with the general trend of opinions regarding Washington lawmakers and the rise of partisanship narrative prevalent in other scholarly works. The combined of Figures 12 and 13 is that respondents fear partisanship on the intelligence committees more than any other obstacles to effective oversight. Ensuring a strong bipartisan spirit and message exists among committee members appears a critical component to the perception of effectiveness.

Figure 14 reinforces the perception of partial oversight effectiveness, but adds a caveat that the intelligence committees were unlikely capable of preventing intelligence community abuses. The cumulative scale questions depicted in Figure 10 indicate a

plurality of respondents perceived oversight to be more effective than ineffective. Respondents also leaned towards trusting the information provided by the intelligence committees, another positive measure of effectiveness. However, respondents also indicated they had a low level of confidence in overseers' ability to prevent IC abuses. This negative measure of effectiveness was significant because positive measures of overseers' intentions did not lead to a belief in their capability. These results reinforce indications regarding respondent support for powerful centralized oversight institutions.

Figure 14. Perceptions of Effectiveness



Overall, the results suggest respondents perceived intelligence oversight by Congress to be effective, but added important caveats. There were multiple positive indicators of effectiveness across question types. Two questions directly asked for assessments of effectiveness while respondents also indicated they trusted information

from the intelligence committees. There were positive indicators of intelligence committee intentions to be effective through a desire to protect civil liberties, but a lower level of confidence in their ability to do so. In addition, the results reinforced the perception that partisanship was the most significant obstacle to effective oversight. This implies respondents believe the path to effectiveness starts with bipartisanship.

A Holistic Assessment of Oversight. The data assessed together provides complementary assessments of the significance, structure and effectiveness of intelligence oversight. Respondents indicated their general belief in the importance of the intelligence committees and then consistently supported the structure and effectiveness of oversight institutions with positive measures of success. In addition, the lower confidence in oversight capabilities was consistent with the indicators for changes in oversight structure, particularly increased centralization. The importance of bipartisanship for effective oversight is underscored in the diversity of responses given for the purpose of intelligence oversight.

The survey demonstrated the perception that current oversight institutions are important to respondents, but some structural changes are needed to improve overall effectiveness. Translating the results into action, committee members could use current intelligence salience as a springboard for needed changes in committee structure. The results also serve as a counterargument to advocates for major upheaval to intelligence oversight as a result of the recent NSA collection controversy. In fact, respondents in the survey suggested some level collection on U.S. citizens was permissible, which leads to several additional questions outside the scope of this research. Related to this paper

however, greater collection freedom for the IC reinforces the need for engaged intelligence oversight.

The survey and its results cannot be applied to the entire American citizenry, but the results can serve to foster reconsideration of notions regarding perceptions of intelligence oversight. Additionally, because the survey included government officials with ties to the intelligence committees' staff the results provide an undetermined amount of self-critique. The results indicate that many of the individuals tasked with oversight responsibilities recognize the obstacles and shortcomings. Overseers might endorse needed shifts in responsibility or structural adjustments in order to improve effectiveness. The recognition of obstacles among insiders should serve as a source of reassurance to those who assume intelligence overseers are ignorant of inherent shortfalls.

CONCLUSION

The results of this research suggest the trust in intelligence oversight among informed respondents is not lost. In a nuanced fashion, it contradicts many prevailing public opinion polls that indicate a major loss of confidence in Congress. This is critical because the IC, more than any other government institution, relies on trust for resources and validation. The segment of the population analyzed in this study is the least likely to lose trust IC oversight, however they also would sound the loudest alarm yet for needed reform if the results had indicated otherwise. The secrecy inherent to the IC mission requires people to trust the institutional arrangement of the community and those designated to oversee it. Without trust in the IC, the U.S. government would have a fundamental contradiction between its core values and the institutions designed to uphold those values. If the results of the survey followed general trends for confidence and trust

in Congress then the IC would be on "thinning ice" in its mission to defend the nation. In contrast, the results indicate there is an understanding and appreciation of the IC and its overseers. Respondents in the survey expressed concerns, but reinforced the most important foundations for congressional oversight institutions. Even for policy areas less attractive for electoral success it is important that lawmakers take stock of opinions regarding government effectiveness. Perceptions of intelligence oversight provide valuable indicators for legislator's stewardship of America's most grave institutions.

THE FINAL CROSSING

"Voting for National Security," outlined the changing trends among SSCI membership since the committee's inception in 1976. There is considerable scholarship devoted to assessing the effects of partisanship on the SSCI and a common assumption among researchers that partisanship is rising. A key significance of this supposed rise is the reduced likelihood the IC will cooperate with intelligence overseers. The protection of sources and methods to provide policymakers a strategic advantage leads to a substantial amount of secrecy in the IC. In order to access relevant information to perform their oversight duties, SSCI members need a cooperative relationship with the IC. Broken trust between the IC and the SSCI leaves congressional overseers in the precarious position of trying to oversee the community without all the pertinent information. The recent public clashes between CIA Director Brennan and SSCI Chairwoman Feinstein could easily lead to a much more challenging oversight environment for the SSCI.[209]

The SSCI is one of only a few external IC oversight institutions, if it fails to provide effective oversight there are few alternatives. The IC does not traditionally garner high public salience levels, which means it is easy for the community to conduct its business without public inquiry into impropriety. There are few constituency groups that can effectively provide oversight given the limited publically available information, which adds significance to the SSCI's oversight responsibilities. However, overseers struggle with competing demands for time and few electoral incentives for emphasis on intelligence oversight. Add to this mix the possibility of rising partisanship within a historically bipartisan environment and the results for effective intelligence oversight are strongly negative.

[209] Mark Mazzetti, "C.I.A. Inquiry is Set in Clash on Detentions," *New York Times*, sec. A1: 5 Mar 2014.

Chapter one identified a modestly rising partisan membership within the SSCI based on dynamic-weighted nominate scores. Both political parties are increasingly assigning members who arrive to the SSCI with stronger partisan leanings then their predecessors. In addition, the data suggests SSCI voting trends are becoming more partisan. There is not a consistent rise "yea" vote differences between Democrats and Republicans however, there is more dramatic party unity on certain votes. This suggests that in certain circumstances, for instance highly political issues, SSCI members are trending away from bipartisan votes and voting along party lines.

These trends do not directly lead to ineffective oversight. In some cases, increased partisanship within the SSCI could lead to more investigative, "police patrolling" type oversight during periods of divided government. However, the data also suggests that periods of divided government do not necessarily lead to increases in partisan voting. On the contrary, periods of undivided government contained greater "yea" vote differences then periods of divided government. The data suggests that partisanship is modestly increasing, but the effects of that rising partisanship remain to be seen. Chapter one studied the aggregate over thirty years, while reviewing rhetoric in a case study approach, such as Chapter two, provided a slightly different perspective.

Changing membership and vote trends are not the only source of evidence regarding bipartisanship in the SSCI. Chapter two's case study in cyber domain oversight explored the challenges associated with protecting civil liberties while simultaneously considering national security implications and providing effective oversight. As the threat of cyber attack and terrorism unfolded in the early part of the twenty-first century the SSCI was confronted with oversight challenges regarding

effective use of American technological advantage to thwart terrorist attacks, prevent cyber attacks and conduct operations in cyber space.

Although the cyber domain consistently drew the attention of SSCI members throughout hearings in the 2000s, challenges with digital security and privacy dated as far back as the 1960s. The series of hearings examined in "The Cyber Domain," focused on a multitude of issues related to long-standing questions surrounding IC cyber activities. The SSCI was assessed on its ability to provide the IC strategic guidance, actively legislate, ensure the IC adhered to constitutional principles, and educate the public. Open hearing dialogue for annual threat hearings and specialized hearings was available to supply evidence of the SSCI oversight effectiveness.

The results of "The Cyber Domain," suggest the committee actively approached its oversight responsibility and created a bipartisan atmosphere in open hearings. The data suggests there is a slight trend towards decreased participation in open hearings in the last ten years however, the committee consistently garnered at least 50 percent participation in its open hearings. Additionally, both political parties demonstrated regular participation, although the party in control of the Senate consistently received better participation from its members. Annual threat hearings in the last ten years contained inconsistent approaches to cyber oversight by the SSCI. The SSCI provided useful public advocacy through open threat hearings, but was less successful at providing the IC strategic cyber guidance. This manifested itself mainly through an inability to relate the interconnected nature of foreign cyber threats facing the U.S. and the tools used domestically to combat terrorism. In targeted hearings over the last ten years the trend was opposite. SSCI members focused heavily on constitutional adherence over

controversial topics like FISA or the USA PATRIOT Act. However, SSCI members were not legislatively active enough or forward thinking enough to provide effective strategic guidance to the IC. Despite nuanced shortcomings committee members were strongly engaged on all these critical issues, indicative of an active oversight committee that was investigating critical issues surrounding the IC.

Chapter three explored the public's perceptions of intelligence overseers. In contrast to the earlier two chapters, "If Angels Were to Govern Men" broadened the scope of research to all congressional oversight of intelligence. Focusing on only the SSCI in a public opinion survey would have been too specific to extract useful results. However, public perceptions of congressional intelligence oversight have an important role in IC policy. Public opinion is proven to have an effect on legislators, even in less salient policy areas such as intelligence. In addition, the IC and its overseers rely on the public's trust to operate in secret. The IC also relies on overseers to provide the necessary funds and resources to assist the community in providing policymakers a distinct strategic advantage against the U.S.'s adversaries. These two factors leave a strong impetus for legislators to take stock in the public's opinions of intelligence oversight, even if those opinions are not nuanced about the details of all intelligence policy.

"If Angels Were to Govern Men," used a public opinion survey to gather perceptions regarding intelligence oversight. It is important to reiterate that the survey results do not represent the American populace. However, the results do represent an informed segment of the population with knowledge and understanding of national security policy. Respondents provided strong indicators in support of current oversight

institutions and a hands-on approach to intelligence oversight. Respondents were also far less protective of privacy then expected, especially in light of the recent revelations concerning NSA bulk data collection. The survey also indicated generally positive opinions of oversight structures and effectiveness, contradicting prevailing opinions regarding Congress writ large. The survey results suggest that if partisanship is rising and if oversight effectiveness has shortfalls, the public's perception of intelligence oversight is not significantly degraded by those two detractions.

It is plausible that partisanship has not reached such a height that it draws negative attention towards intelligence overseers. However, the data consistently provided positive indicators of at least partial effectiveness. In addition, the survey was conducted in the midst of leaks by NSA contractor Edward Snowden regarding bulk data collection. Leaked classified information and data collection easily construed as invading privacy suggested perceptions of oversight would be negative. Despite the negative publicity, intelligence overseers still received several positive indicators for effectiveness and the belief that only mild changes were needed in intelligence oversight.

THINGS ARE NOT WHAT THEY SEEM

All three chapters of *Crossing the Rubicon* provided mixed results concerning the SSCI and intelligence oversight. Negative trends in partisan membership and voting suggested the SSCI was heading towards obstacles in its relationship with the IC and degraded effectiveness. In contrast, a close examination of the cyber domain suggested partisanship was not significantly influencing oversight while instead issue complexity and the topic du jour was inhibiting continuous focus on an emerging cyber threat. Finally, none of those shortfalls were severe enough to significantly alter public opinion

of intelligence oversight. Public perceptions of oversight were more positive then the rest of Congress and a variety of positive indicators suggested no more then mild changes were required to improve oversight.

The results reiterate a conclusion from chapter two regarding SSCI oversight in the cyber domain. Overall, intelligence oversight has many shortfalls and obstacles to success, however there is no evidence the committee is ignorant or irreverent of the important role intelligence oversight plays in protecting the U.S. and its ideals. The results suggest SSCI members understand their important governmental function, which is necessary to ensure policymakers are informed; institutions function as designed, and resources are allocated properly. This conclusion is immensely important when considering the SSCI in the context of a viable oversight institution meeting its intended role. The evidence does not support significant overhaul is needed to congressional oversight structures. The evidence in all three chapters reinforces the committee's importance to the IC and the American public.

Partisanship matters and if it continues to increase the results are likely to be negative for the IC, the public, and the SSCI. "The Cyber Domain," presented some positive evidence of bipartisanship within the SSCI. However, chapter one provided evidence that overall partisan levels are likely rising, albeit slowly. In addition, "If Angels Were to Govern Men," added public perceptions regarding the negative effects associated with rising partisanship. Overall, the inability of other external actors to provide effective oversight leaves the impetus on congressional overseers to operate above traditional politics and find consensus in order to strengthen trust with the IC and the citizenry. Senate Resolution 400 from the 94th Congress states, "the majority leader

shall appoint the majority members and the minority leader shall appoint the minority members, with the majority having a one vote margin."[210] It was designed to be a bipartisan committee in order to address intelligence oversight pragmatically vice politically.

Intelligence oversight must find avenues to provide persistent oversight of programs and policies related to emerging threats. A challenge for the IC, as well as the SSCI, is to not always be reactive to crises. Legislators must dedicate time to revisiting issues beyond the topic du jour that are addressed in annual threat briefings or targeted hearings. Finding methods to persistent coverage of unanticipated issues will assist the SSCI in providing better strategic guidance to the IC on challenges such as cyber domain boundaries for electronic surveillance. The issue of today might be terrorism or NSA collection programs, but the issues of tomorrow's IC could be resource shortages and demographics that cause political instability. The SSCI's guidance and vision will help establish IC priorities and boundaries.

Public opinion matters, even in intelligence oversight where it takes unique access to examine the IC. Perceptions of the committee are essential to the underlying trust between Americans and their government. Committee members should pay keen attention to public opinions because over the long term those opinions will directly affect the SSCI's ability to provide resources to the IC. The IC must prioritize human and technological resources and the SSCI has a critical role in ensuring public support for those investments. Chapter three indicates that a well-informed portion of the population remains supportive of intelligence oversight institutions. Further research could uncover

[210] Senate Select Committee on Intelligence, *Rule of Procedure for the Select Committee on Intelligence United States Senate 112th Congress* (Washington: U.S. Government Printing Office, 2011), 14.

if that perception extends more broadly across the U.S. Either way, committee members should reflect upon any available public perceptions of oversight effectiveness in order to better represent the primary constituency for the SSCI, the American public.

Crossing the Rubicon does not uncover any unfounded truths to intelligence oversight. It attempted to examine oversight methodically and objectively to better understand an important component in the U.S. national security apparatus. The IC faces enormous challenges to provide strategic warning and prevent strategic surprise. A vast number of dedicated individuals make up the IC, but the good intentions and momentum of any large bureaucracy can lead it astray. The SSCI, HPSCI and other executive branch oversight entities have critical responsibilities to ensure the IC operates within its prescribed boundaries. The ideals that form the foundation for America demand intelligence overseers always remain inquisitive and vigilant.

BIBLIOGRAPHY

Aberbach, Joel D. "Changes in Congressional Oversight." *The American Behavioral Scientist* 22.5 (1979): 493-515.

Adams, James. "Virtual Defense." *Foreign Affairs* 80, 3 (2001): 98-112.

Balnaves, Mark, and Peter Caputi. *Introduction to Quantitative Research Methods: An Investigative Approach*. London: Sage Publications, 2001.

Blum, Stephanie Cooper. "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." *BU Pub. Int. LJ* 18 (2008): 269-314.

Brady, Henry E. "Contributions of Survey Research to Political Science." *Political Science and Politics* 33, 1 (2000): 47-57.

Burstein, Paul. "The Impact of Public Opinion on Public Policy: A Review and an Agenda." *Political Research Quarterly* 56, 1 (2003): 29-40.

Carroll, Royce and Jeffrey Lewis, et. al. DW Nominate Scores, 1st to 111th Congresses, Senate, 94th to 111th Congresses, February 3, 2011, <http://voteview.com/dwnominate.asp> (accessed March 4, 2012).

Carroll, Royce and Jeffrey Lewis, et. al. *"Measuring Bias and Uncertainty in DW-NOMINATE Ideal Point Estimates via the Parametric Bootstrap,"* Political Analysis 17 (2009): 261-275. (accessed March 15, 2012).

Cavelty, Myrium D. and Victor Mauer. "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence." *Strategic Dialogue* 40 (2009): 123-144.

Clapper, James R. "Worldwide Threat Assessment of the U.S. Intelligence Community." Statement for the Record, Senate Select Committee on Intelligence, Washington D.C., March 12, 2013.

Colton, David Everett. "Speaking Truth to Power: Intelligence Oversight in an Imperfect World." *University of Pennsylvania Law Review* 137, 2 (1988): 571-613.

Ellis, James, David Fisher, Thomas Longstaff, Linda Pesante and Richard Pethia. *Report to the President's Commission on Critical Infrastructure Protection*. Pittsburgh: Carnegie Mellon University, 1997.

George, Alexander L. "Case Studies and Theory Development: The Method of Structured, Focused Comparison." In *Diplomacy: New Approaches in History, Theory, and Policy,* edited by Paul Gordon Lauren, 43-68. New York: The Free Press, 1979.

Gellman, Barton and Laura Poitras. "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program." *The Washington Post*, June 6, 2013.

Glees, Anthony & Philip H.J. Davies. "Intelligence, Iraq and the limits of legislative accountability during political crisis." *Intelligence and National Security* 21 no. 5 (2006): 848-883.

Goel, Sanjay. "Cyberwarfare: Connecting the Dots in Cyber Intelligence." *Communications of the ACM* 54, 8 (2011): 132-140.

Gorman, Siobahn, Evan Perez, and Janet Hook. "U.S. Collects Vast Data Trove." The *Wall Street Journal*, June 7, 2013.

Greenwald, Glenn. "NSA collecting phone records of millions of Verizon customers daily." *The Guardian*, June 5, 2013.

Hartley, Thomas and Bruce Russert. "Public Opinion and the Common Defense: Who Governs Military Spending in the United States?" *The American Political Science Review* 86, 4 (1992): 905-915.

Hass, Douglas A. "Crafting Military Commissions Post-Hamdan: The Military Commissions Act of 2006." *Indiana Law Journal* 82 (2007): 1101-1124.

H.R. 3523--112th Congress: Cyber Intelligence Sharing and Protection Act." www.GovTrack.us. (2011): http://www.govtrack.us/congress/bills/112/hr3523 (accessed 6 April 2014).

Hughes, R. Gerald, and Kristan Stoddart. "Hope and Fear: Intelligence and Global Security a Decade after 9/11." *Intelligence and National Security* 27, 5 (2012): 625-652.

Jacobs, Lawrence R., Eric D. Lawrence, Robert Y. Shapiro, Steven S. Smith. "Congressional Leadership of Public Opinion." *Political Science Quarterly* 113, 1 (1998): 21-41.

Johnson, Loch K. *A Season of Inquiry: Congress and Intelligence*. Chicago: Dorsey, 1988.

Johnson, Loch K. "Accountability and America's Secret Foreign Policy: Keeping a Legislative Eye on the Central Intelligence Agency." *Foreign Policy Analysis* 1 (2005): 99-120.

Johnson, Loch K. "Ostriches, Cheerleaders, Skeptics, and Guardians: Role Selection by [US] Congressional Intelligence Overseers." *SAIS Review of International Affairs* 28 no. 1 (2008): 93-108.

Johnson, Loch K. “The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability.” *Intelligence and National Security* 23, 2 (2008): 198-225.

Kerr, Orrin S. “A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It.” *George Washington Law Review* 72, 6 (2004). http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1706&context=faculty_publications&seiredir=1&referer=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fhl%3Den%26q%3Delectronic%2Bcommunications%2Bprotection%2Bact%26btnG%3D%26as_sdt%3D1%252C21#search=%22electronic%20communications%20protection%20act%22 (accessed 4 August 2013).

Kerr, Orin S. “Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't.” *Northwestern University Law Review* 97 (2003): 607-674. http://ssrn.com/abstract=317501 or http://dx.doi.org/10.2139/ssrn.317501 (accessed 14 July 2013).

Kibbe, Jennifer. “Congressional Oversight of [US] Intelligence: Is the Solution Part of the Problem?.” *Intelligence and National Security* 25 no. 1 (2010): 24-49.

Knott, Stephen F. “The Great Republican Transformation on Oversight.” *International Journal of Intelligence and CounterIntelligence* 13 no. 1 (2000): 49-63.

Lee, Frances E. “Party Politics and the Permanent Campaign on the Senate Floor.” Paper presented at the University of Maryland American Politics Workshop, February 18, 2011.

Liu, Edward C. “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015.” Congressional Research Service, Library of Congress, 2012.

Lorber, Eric. “Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?” *University of Pennsylvania Journal of Constitutional Law* 15, 3 (2013): 961-1002.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 4th ed. Washington DC: CQ Press, 2009.

Lowi, Theodore and Benjamin Ginsberg, et. al. *American Government: Power and Purpose,* Eleventh Ed. New York, NY: Norton, 2010.

Lynn III, William J. “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs* 89, 5 (2010): 97-108.

Madison, James. "The Federalist No. 51." Web. <http://www.constitution.org/fed/federa51.htm>.

Matei, Florina Christiana and Thomas Bruneau. “Policymakers and Intelligence Reform in New Democracies.” *International Journal of Intelligence and Counterintelligence* 24 (2011): 656-691.

Mazzetti, Mark. "C.I.A. Inquiry is Set in Clash on Detentions." *New York Times*, sec. A1: 5 Mar 2014.

McCarthy, Gregory C. “GOP Oversight of Intelligence in the Clinton Era.” *International Journal of Intelligence and Counterintelligence* 15 no.1 (2002): 26-51.

McConnell, Mike. “Mike McConnell on How to Win the Cyber War We are Losing.” *The Washington Post*, February 28, 2010.

Nelson, Garrison. Committees in the U.S. Congress, 1947-1992, Senate, 94th to 102nd Congresses, March 10, 2008, <http://web.mit.edu/17.251/www/data_page.html#0> (accessed March 4, 2012).

Page, Benjamin I. and Robert Y. Shapiro. “Effects of Public Opinion on Policy.” *The American Political Science Review* 77, 1 (1983): 175-190.

Pew Research Center. *Distrust, Discontent, Anger and Partisan Rancor: The People and Their Government*. Washington, DC: Pew Research Center for the People and the Press, 2010.

Pew Research Center. *Majority Says the Federal Government Threatens Their Personal Rights: Views of Congress*. Washington, DC: Pew Research Center for the People and the Press, 2013.

Pew Research Center for the People and the Press. “Methodology.” < http://www.people-press.org/methodology/> (accessed August 27, 2013).

Ott, Marvin C. “Partisanship and the Decline of Intelligence Oversight.” *International Journal of Intelligence and CounterIntelligence* 16 no. 1 (2003): 69-94.

Rizzo, John. “The CIA-Congress War.” *Defining Ideas* (2012): http://www.hoover.org/publications/defining-ideas/article/112491 (accessed June 15, 2013).

Ron Wyden Senator for Oregon. “Bipartisan Group of 26 Senators Seek Answers from DNI Clapper and Bulk Data Collection Platform.” http://www.wyden.senate.gov/news/press-releases/bipartisan-group-of-26-senators-seek-answers-from-dni-clapper-on-bulk-data-collection-program (accessed July 29, 2013).

Schlesinger, Joseph A. “The New American Political Party.” *The American Political Science Review* 79 no. 4 (1985): 1152-1169.

Schmitter, Phillipe C., and Terry Lynn Karl. "What Democracy is...and is Not." *Essential Readings in Comparative Politics.* Eds. Patrick H. O'Neil and Ronald Rogowski. 4th ed.WW Norton & Company Inc., 2006. 204-217.

Senate Select Committee on Intelligence. *Attorney General Guidelines for FBI Criminal Investigations, National Security Investigations, and the Collection of Foreign Intelligence* S. Hrg 110-846. Washington: U.S. Government Printing Office, 2008.

Senate Select Committee on Intelligence. *Congressional Oversight of Intelligence Activities* S. Hrg 110-794. Washington: U.S. Government Printing Office, 2007.

Senate Select Committee on Intelligence. *Congressional Oversight of Intelligence Activities* S. Hrg 110-794. Washington: U.S. Government Printing Office, 2007.

Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States* S. Hrg 108-588. Washington: U.S. Government Printing Office, 2004.

Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States* S. Hrg 109-61. Washington: U.S. Government Printing Office, 2005.

Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States* S. Hrg 109-724. Washington: U.S. Government Printing Office, 2006.

Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States* S. Hrg 110-835. Washington: U.S. Government Printing Office, 2007.

Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States* S. Hrg 110-824. Washington: U.S. Government Printing Office, 2008.

Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States* S. Hrg 111-62. Washington: U.S. Government Printing Office, 2009.

Senate Select Committee on Intelligence. *Current and Projected National Security Threats to the United States* S. Hrg 111-557. Washington: U.S. Government Printing Office, 2010.

Senate Select Committee on Intelligence. “Current and Projected National Security Threats to the United States.” Hearing before the Select Committee on Intelligence of the United States Senate held on February 16, 2011.

http://congressional.proquest.com/congressional/docview/t65.d40.02160003.s32?accountid=11752 (accessed 7 July 2013).

Senate Select Committee on Intelligence. "Current and Projected National Security Threats to the United States." Hearing before the Select Committee on Intelligence of the United States Senate held on March 12, 2013. http://congressional.proquest.com.proxy3.library.jhu.edu/congressional/docview/t65.d40.03120003.s37?accountid=11752 (accessed 7 July 2013).

Senate Select Committee on Intelligence. *Intelligence Reform* S. Hrg 110-839. Washington: U.S. Government Printing Office, 2007.

Senate Select Committee on Intelligence. *Intelligence Community Reform* S. Hrg 108-656. Washington: U.S. Government Printing Office, 2004.

Senate Select Committee on Intelligence. *Modernization of the Foreign Intelligence Surveillance Act* S. Hrg 110-399. Washington: U.S. Government Printing Office, 2007.

Senate Select Committee on Intelligence. *Reform of the United States Intelligence Community* S. Hrg 108-835. Washington: U.S. Government Printing Office, 2004.

Senate Select Committee on Intelligence. *Rule of Procedure for the Select Committee on Intelligence United States Senate 112th Congress*. Washington: U.S. Government Printing Office, 2011.

Senate Select Committee on Intelligence. "Sen. Dianne Feinstein and Rep. Mike Rogers Hold a Joint Hearing on the State of Intelligence Reform." Hearing before the Select Committee on Intelligence of the United States Senate held on September 13, 2011. http://congressional.proquest.com.proxy3.library.jhu.edu/congressional/docview/t65.d0.09130003.s66?accountid=11752 (accessed June 24, 2013).

Senate Select Committee on Intelligence. *Statutory Authorities of the Director of National Intelligence* S. Hrg 110-837. Washington: U.S. Government Printing Office, 2008.

Senate Select Committee on Intelligence. *The Federal Bureau of Investigation's Strategic Plan and Progress on Reform* S. Hrg 110-793. Washington: U.S. Government Printing Office, 2007.

Senate Select Committee on Intelligence. *USA Patriot Act* S. Hrg 109-341. Washington: U.S. Government Printing Office, 2005.

Smist, Frank J. *Congress Oversees the United States Intelligence Community, 1947-1993*. 2nd ed. Knoxville: The University of Tennessee Press, 1994.

Snider, L. Britt. *The Agency and the Hill : CIA's Relationship with Congress*, 1946-2004. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2008.

Snider, L. Britt. *Sharing Secrets with Lawmakers: Congress As a User of Intelligence*. Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 1997.

Stewart III, Charles and Jonathan Woon. Congressional Committee Assignments, 103rd to 112th Congresses, 1993--2011: Senate, April 12, 2011, <http://web.mit.edu/17.251/www/data_page.html#0> (accessed March 4, 2012).

The U.S. National Archives & Records Administration. *The Constitution of the United States: A Transcription*., September 17, 1787.

Turabian, Kate L. *A manual for writers of research papers, theses, and dissertations: Chicago style for students and researchers*. University of Chicago Press, 2013.

U.S. House Resolution 2647--111th Congress. *"National Defense Authorization Act for Fiscal Year 2010."* GovTrack.us (database of federal legislation). (2009): <http://www.govtrack.us/congress/bills/111/hr2647> (accessed April 5, 2012).

U.S. House Resolution 3162--107th Congress. *"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001."* GovTrack.us (database of federal legislation). (2001): <http://www.govtrack.us/congress/bills/107/hr3162> (accessed April 4, 2012).

U.S. House Resolution 3604--110th Congress. *"FISA Amendments Act of 2008."* GovTrack.us (database of federal legislation). (2008): <https://www.govtrack.us/congress/votes/110-2008/s168> (accessed March 14, 2014).

U.S. Senate Joint Resolution 44--104th Congress. *"A joint resolution concerning the deployment of U.S. Armed Forces in Bosnia-Herzegovina."* GovTrack.us (database of federal legislation). (1995): <http://www.govtrack.us/congress/bills/104/sjres44> (accessed June 3, 2013).

U.S. Senate Resolution 2845--108th Congress. *"Intelligence Reform and Terrorism Prevention Act of 2004."* GovTrack.us (database of federal legislation). (2004): <http://www.govtrack.us/congress/bills/108/s2845> (accessed April 4, 2012).

U.S. Senate Resolution 3930--109th Congress. *"Military Commissions Act of 2006."* GovTrack.us (database of federal legislation). (2006): <https://www.govtrack.us/congress/votes/109-2006/s259> (accessed March 14, 2014).

U.S. Senate Resolution 4--110th Congress. *"Improving America's Security Act of 2007."* GovTrack.us (database of federal legislation). (2007): <http://www.govtrack.us/congress/bills/110/s4> (accessed April 18, 2012).

U.S. Senate Resolution 1927--110th Congress. *"Protect America Act of 2007."* GovTrack.us (database of federal legislation). (2007): <http://www.govtrack.us/congress/bills/110/s1927> (accessed April 18, 2012).

U.S. Senate Select Committee on Intelligence. "Members, Publications, Legislation." <http://intelligence.senate.gov/index.html> (accessed March 4, 2012).

Van Wagenen, James S. "A Review of Congressional Oversight." *Studies in Intelligence* 40, no. 5, (1997): 97-102. URL <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA524502&Location=U2&doc=GetTRDoc.pdf> (accessed 14 February 2012).

Verba, Sydney. "The Citizen as Respondent: Sample Surveys and American Democracy Presidential Address, American Political Science Assocation 1995." *The American Political Science Review* 90, 1 (1996): 1-7.

Walker, Matthew B. "Reforming Congressional Oversight of U. S. Intelligence." *International Journal of Intelligence and Counterintelligence* 19, no. 4 (2007): 702-720.

Warner, Michael. "Cyber Security: A Pre-History." *Intelligence and National Security* 27, 5 (2012): 781-799.

Zegart, Amy & Julie Quinn. "Congressional Intelligence Oversight: The Electoral Disconnection." *Intelligence and National Security* 25 no. 6 (2010): 744-766.

Zegart, Amy. "The Domestic Politics of Irrational Intelligence Oversight." *Political Science Quarterly* 126 no. 1 (2011): 1-25.

Curriculum Vita: Ralph W. Corey was born on September 27th 1983 in Farmington, Minnesota. He has a Bachelor of Arts in Political Science from Norwich University. He is an Intelligence Officer in the United States Navy currently assigned to U.S. Pacific Command. He has previously deployed in support of Operation Iraqi Freedom and Operation Enduring Freedom.