

The Cyber-Industrial Complex

Connor O'Malley
Bemidji State University

Political Science Senior Thesis
Bemidji State University
Dr. Patrick Donnay, Advisor
April 2016

Abstract

When Edward Snowden released a massive trove of classified files from the National Security Agency, the world became aware of numerous global surveillance systems. As Snowden hoped, a global dialogue began concerning surveillance, privacy, and government transparency. While there was a lively discourse surrounding the leak and Snowden, another story was missed. Snowden was not an employee of the NSA; rather he was an employee of Booz Allen Hamilton, a private contractor maintaining computer systems for the NSA. The deeper story here is the emerging relationship between government agencies and technology companies.

This paper discusses the theory of iron triangles and issue-networks, specifically the issue networks within the United States Intelligence community. The aim of an issue network is to shape policy outcomes, therefore I will examine the connection between Congress, intelligence agencies, and the private companies involved in the cyber-industrial complex. I hypothesize that senators receiving campaign contributions from intelligence contractors are more likely to vote in favor of surveillance activities. I use campaign data from the Center for Responsive Politics from 2009-2014, and Senate votes during the 114th Congress. My findings show there is a complex relationship between lobbying, intelligence spending, and the voting behavior of the Senate.

Introduction

From time to time, there are events that provide insight into the very secretive world of the United States Intelligence Community. For obvious reasons, the activities of this community take place largely in the shadows, outside the visible political world. This secrecy is intended to be a safeguard against those who wish to do harm to the United States. At the same time however, this secrecy also insulates the Intelligence Community (IC) from oversight and accountability. While we hope that the IC is acting in our best interest, the public lacks the classified information needed to confirm that they are. In the summer of 2013, some of that information leaked into the public forum and ignited a global conversation about government surveillance.

One part of this conversation deals with the nature of the relationship between intelligence agencies and the private contractors they employ. Many of the functions of the National Security Agency (NSA) and Central Intelligence Agency (CIA) have been outsourced to the private sector. Edward Snowden, the source of the 2013 NSA leaks, downloaded the classified material while he was an employee of the private contractors Booz Allen Hamilton and Dell. The fact he was able to accumulate this information while not officially being employed by the NSA, shows just how intertwined private contractors are in the world of surveillance.

This paper seeks to further examine this relationship between US intelligence agencies and private contractors. It will attempt to explain this relationship using the policy theories of both Iron Triangles and Issue Networks. While there is extensive literature on these theories, they have not yet been applied to the intelligence establishment. I will argue that elements of

both policy making models are present in the current United States Intelligence Community.

This paper will also discuss the ongoing privatization of the US intelligence operations and the effects that it may have on the formulation of policy.

Literature Review

Edward Snowden and The NSA Surveillance

Edward Joseph Snowden was identified as the source of the NSA leaks. He was able to obtain this information while he was working for Dell and Booz Allen Hamilton, who were under contract with the NSA (Greenwald, 2014) (Ray, 2015). Snowden's career in the IC officially began in 2005 when his abilities with computers landed him a position as a technical expert for the Central Intelligence Agency with "Top Secret" security clearance. In 2009 he left the CIA for the NSA, and began his work as a systems administrator for Dell and Booz Allen Hamilton. From this position Snowden had a very high level of access to the surveillance activities of the NSA. Throughout 2012, he downloaded the trove of files that would eventually be leaked. On June 5th 2013 the newspaper *The Guardian* began publishing the numerous stories based on Snowden's files (Greenwald, 2014). The leaks revealed a massive surveillance apparatus, with the ability to monitor communications on a global scale. Programs and tools like PRISM and BOUNDLESS INFORMANT were suddenly ripped from the shadows and became front-page news.

PRISM was a program that began in 2007 through which the NSA had access to the servers of nine major telecommunications companies in the United States. According to a leaked NSA document, "PRISM collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, Youtube" (Greenwald

2014, 108). “Collection Details varies by provider: email, chat-video, voice, photos, stored data, VoIP, file transfers, video conferences, notification of login information, social network activity, special requests” (Greenwald 2014,). “According to a partially declassified 2011 opinion from the Foreign Intelligence Surveillance Court (FISC), NSA collected 250 million Internet communications per year under this program. Of these communications, 91% were acquired —directly from Internet Service Providers, referred to as —PRISM collection.” (Liu 2014)

The Metadata programs, also known as the “telephony data programs”, involved the NSA compelling telephone companies to turn over huge volumes of call data (Peterson, 2013). The first story that broke concerned the request from the NSA to Verizon to turn over the data from all US customers, nearly 120 million people (Greenwald, 2014). “One program collects in bulk the phone records—specifically the number that was dialed from, the number that was dialed to, and the date and duration of the call—of customers of Verizon Wireless and possibly other U.S. telephone service providers. It does not collect the content of the calls or the identity of callers (Erwin 2013).

BOUNDLESS INFORMANT (BI) was a tool used to access the information collected from the metadata programs, upstream collection programs, and through PRISM (Greenwald & MacAskill, Boundless Informant: the NSA's secret tool to track global surveillance data, 2013). BI organized the huge amounts of raw surveillance data into organized categories, for instance by country. This revelation was significant because it proved that the NSA kept detailed records on the volumes of data collected, contrary to what Director James Clapper told Congress in an oversight hearing. According to BI, “overall in just thirty days the unit [Global Access

Operations] had collected data on more than 97 billion emails and 124 billion phone calls from around the world (Greenwald 2014).

The legal justification for these programs comes from a combination of legislation including the Foreign Intelligence Surveillance Act of 1978 (FISA 1978), Section 215 of The PATRIOT ACT, and Executive order 12333. The FISA 1978 outlined a surveillance system very different than our current one, and created the FISA Court (Federal Judicial Center, n.d.). It was much more similar to law enforcement investigations in the sense that the IC would be required to submit a request for targeted surveillance to a FISA Court for approval (Liu, 2014). Section 215 of the Patriot Act amended this section of FISA to loosen the requirements of submissions to the FISA court for approval, thus enabling the domestic bulk collection data programs leaked by Snowden. Executive Order 12333 creates a distinction between the necessary procedures for an “investigation” rather than what is known as a “threat assessment”. An investigation implies that there is evidence that a target is already a threat and further surveillance information is needed in order to guarantee security, ordinarily an investigation would require a visit to the FISA Court, however, by broadening the definition of a “threat assessment” the IC was able to conduct surveillance that normally would be considered an “investigation” (Erwin, 2013).

Iron Triangles and Issue Networks

In January of 1961, President Dwight D. Eisenhower delivered his famous *Farewell Address to the Nation*. This speech will always be remembered for its introduction of the term “military-industrial-complex” to describe the close relationship between the arms manufacturers and government since the end of World War II (Eisenhower, 1961). Eisenhower

made sure to identify what he believed to be a potentially dangerous policy making system later known as an Iron Triangle, or sub-government. Many writers will use these terms interchangeably to explain a cooperative relationship similar to the military-industrial-complex. From the theory of Iron Triangles, the further theory of Issue Networks evolved as the relationships became more complex over time. I will be using elements of both to describe the current Intelligence Community.

Iron Triangles are presented as a series of close relationships between an executive agency, the relevant congressional committee, and an interest group, to achieve a communal goal (Hecl, 1978) (Ginsberg, 2013). Iron triangles are also referred to as “subgovernments” and “subsystems” due to their ability to expedite checks and balances of the policy making process. These systems exist when the network of members is small, and their positions in government or business are stable, and all the members agree to cooperate (Jordan, 1981). The small network results in fewer people spending greater amounts of time communicating, which in turn creates informal relationships. Examples of “stable positions” include legislators from safe districts, businesses with long term government contracts, and appointed officers in executive agencies. If these conditions are met, an Iron Triangle is capable of “developing and administering public policy within its narrow realm without significant opposition from elsewhere in the government system” (Gais, 1984).

Using the military-industrial-complex as an example, the Iron Triangle exists between the House and Senate Committees on Armed Services, the Department of Defense, and the defense industry (Ginsberg, 2013). The relationship can involve the circulation of funding, political support, favors, and legislation to serve the interests of those involved. The politicians

in Congress need to be reelected are responsible for bringing federal spending to their districts. The Department of Defense seeks the strongest and most advanced military possible. The defense contractors want to sell their technology and services to the Department of Defense. In order for all of them to accomplish their goals, these groups may form an Iron Triangle. The Legislators have control over the federal budget, giving them the ability to increase or decrease funding flowing to the executive agencies. They also have the ability to introduce and vote on legislation that the other members of the triangle must abide by. The Department of Defense has control over which projects are pursued and which defense companies will receive the contracts for them. In turn the defense contractors can donate to the Legislators' campaigns to help them get reelected. While the Iron Triangle works for explaining the military-industrial-complex, more complex policy issues are better described using Issue Networks.

Issue Networks became the preferred theory for understanding policy formulation after the 1970s to better reflect the changing nature of policy formulation. "The iron triangle concept is not so much wrong as it disastrously incomplete" (Hecklo, 1978). Unlike the Iron Triangle, Issue Networks are far more open, unstable, and unpredictable. The main reason for the shift in the policy process was the drastic increase in political participation by the growing middle class. Through the 1960s and 70s new interest groups were uniting behind the more general political causes for civil rights and environmental protection. By not becoming highly specialized, these new interest groups appealed to a wider audience. These groups brought new voices into the policy process, disrupting the previously closed subsystems and caused them to diversify into issue networks (Gais, 1984). The increased public participation brought many policy issues out of the shadows and into the public eye.

Cyber-Industrial Complex

After examining both Iron Triangles and Issue Networks as models for the policy making process, I would argue that the current IC possesses elements of both models. There seems to be a policy relationship in the IC similar to the military-industrial-complex. Due to the fact that the vast majority of intelligence operations are conducted in secret, the number of members with access to the policy process is limited. The Senate Select Committee on Intelligence, the executive intelligence agencies, and private intelligence contractors are the theoretical legs of what is being called the “cyber-industrial complex (CIC)”. Lacking the proper security clearances to view classified intelligence, those outside of the triangle have very little ability to verify information coming from the IC. Having limited membership is the main characteristic of an Iron Triangle, and allows the members to develop policy without much open discussion or explanation. With the exception of the Senators, most of the parties involved are in “stable” positions within the IC, and as we will see, regularly cross the boundaries between the public and private sectors. The same reasons for cooperation in the military-industrial complex are present in the cyber-industrial complex. Additionally, many of the companies known for producing the planes, tanks, and missiles in the military-industrial complex, and the same companies providing support for intelligence services. However, when the secrecy of their activities is compromised, and the public is allowed into the policy making process, the triangle destabilizes and adopts the characteristics of an Issue Network. Once the public had the resources to participate in the policy discussion, they were able to put pressure on legislators to at least examine the surveillance activities in question.

The Senate Select Committee on Intelligence (SSCI) acts as the legislative branch of the CIC and is tasked with overseeing the intelligence activities of the federal government. The SSCI is made up of 15 senators, 8 from the majority party and 7 from the minority. Two members are taken from each of the Committees on Foreign Relations, Armed Services, Judiciary, and Appropriations. The committee also has four ex officio members, the Majority and Minority leaders, and the Chairman and Ranking member of the Armed Services Committee. (U.S. Senate Select Committee on Intelligence, 2016).

The Senators are all responsible for acting in favor of the national interest, but they also have a responsibility to their home districts to bring home what is known as federal “pork barrel” spending. By lobbying at the federal level to secure contracts and development in their home districts, they can bring jobs and capital to their districts, which in turn makes them more likely to be reelected. When it comes to “pork” the CIC has plenty to go around. For example, when the plans for a new Cyber Command were released, 18 different communities across the country lobbied to become the Command’s new home. Cyber Command promised 10,000 jobs, \$15 billion in government contracts, and millions in new local spending (Jerry Brito, 2011). Orrin Hatch, a previous SSCI member, lobbied directly for his home state Utah to become the new home for the \$1.2 billion data center that promised 6,000 construction jobs, and 200 permanent computer technician positions (Jerry Brito, 2011).

The staff of the SSCI also have access to the policy process. They are responsible for compiling information from hearings, reports, and court rulings and provide it to the committee members for consideration. The committee staff is one location where overlap between the public and private sectors can be seen. In 2014, SSCI Chairman Richard Burr appointed Dr.

Robert Kadlec to Deputy Staff Director for the committee. Previously, Kadlec earned \$451,000 as an “intelligence consultant” that lobbied on behalf of intelligence contractors to the Defense Advanced Research Projects Agency (DARPA) and the NSA (Fang, 2015). Another example of overlap was the appointment of Mathew Pollard to the SSCI staff. Pollard was previously a lobbyist for Orbital Sciences Corporation which provides “space based military and intelligence operations” (Fang, 2015).

The executive branch of the CIC is made up of the many agencies involved in intelligence operations. The agencies that make up the backbone of the IC are the National Security Agency (NSA), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), The Office of Director of National Intelligence (ODNI), The National Reconnaissance Office (NRO), and The National Geo-spatial Intelligence Agency (NGA) (Shorrocks, 2008). Additionally, each branch of the military has its own intelligence agency. Together these agencies are responsible for the collection and analysis intelligence data, and the security of our country’s cyber-infrastructure. These intelligence agencies have become increasingly reliant upon privatization, the delegating of public duties to private organizations (Markusen, 2003). This trend began as a result of the downsizing that took place at the conclusion of the the Cold War. After 9/11, the trend of privatization sped up drastically to accommodate the huge demand for intelligence services to fight the War on Terror (Halchin, 2015). At present, “approximately 70% of our intelligence budget is spent in the private sector” (Halchin, 2015) (Greenwald, 2014). Due to the fact that the details of the Intelligence Budget are classified, this number is estimate among many. The privatization of intelligence operations has created a huge revenue stream that private contractors, some already seen in the military-industrial complex, have capitalized on.

The third leg of CIC is made up of the various private contractors that handle everything from surveillance operations to janitorial services. There are currently as many as 480,000 civilian employees with security clearance employed by over 2,000 companies working for the IC (Goldman, 2013). For this study, the focus will be on a few of the largest contractors in terms of personnel and revenue, as well as some companies that participated in the programs exposed by Snowden. These include: AT&T, BAE Systems, Booz Allen Hamilton, Boeing, General Dynamics, Lockheed Martin, Northrup Grumman, Raytheon, and Verizon.

According to a 2015 Congressional Research report, the jobs that can be outsourced to government contractors are first divided into two categories, “core” and “non-core” personnel. Core personnel are involved in “collection and operations, analysis and production, and enterprise information and technology” require security clearance, and in 2007, made up 27% of the overall IC workforce (Halchin, 2015). This shows how private contractors are an integral part of the intelligence activities of the IC. Contractors are now commonly participating in operations that were previously conducted solely by federal employees or active military members. Additionally, in 2010 the Office of the Director of National Intelligence (ODNI) stated “core contract employees are fundamentally indistinguishable from the US Government employees whose mission they support” (Halchin, 2015).

BAE Systems is an American subsidiary of the British-owned BAE, that is headquartered in Rockville, Maryland. The agencies it has contracts with include the CIA, NGA, NSA, and the ODNI. BAE describes itself as “leading provider of skilled, fully cleared geo-spatial and intelligence analysts”. The subsidiaries directors include General Kenneth Monihan Former Director of the NSA and former Richard J. Kerr Former Deputy Director of the CIA (Shorrock,

2009). Here we see one of the many revolving doors present between the top echelons of the IC and a private contractor involved in intelligence operations.

Booz Allen Hamilton (BAH) is another contracting firm with intimate ties to the IC, headquartered in McLean, Virginia. BAH supports the NSA, ODNI, CIA, NGA, and NRO by providing support for data mining, data analysis, signals intelligence systems engineering, operations support, encryption and decryption, and outsourcing strategy planning (Shorrock, 2008). Mike McConnell, the Executive Vice President of BAH's National Security branch, was the Director of the NSA under President H.W. Bush, and the Director of National Intelligence under President G.W. Bush. While not working the Bush administrations he returned to his position at BAH. (John Foster, 2014) John Clapper, another director of the NSA, was also BAH executive before landing the head job at the NSA (Goldman, 2013)

Boeing is a defense and intelligence contractor headquartered in Chicago, Illinois with offices in Fort Meade, Maryland. Boeing's Intelligence and Security Systems branch has contracts with the NSA, CIA, DIA, NGA, and NRO for "mission infrastructure, intelligence analysis, production, and management of visual geo-spatial information" (Shorrock, 2009). Narus, a subsidiary of Boeing, produces the "fiber optic splitters" required for the NSA's upstream data collection programs. Referenced earlier, upstream collection involves the interception of information by diverting it from the fiber optic cables that link the global communication systems together (Electronic Frontier Foundation, 2013). Boeing also holds a \$2.5 billion contract for a "digital fence" on the U.S.-Mexico border, consisting of integrated sensors, cameras, satellites, to monitor any activity along the border where physical patrols are difficult (Shorrock, 2008).

Lockheed Martin is another contractor present in both the MIC and CIC. Headquartered in Bethesda, Maryland, Lockheed is one of the world's largest private contracting companies. For the CIC, Lockheed has contracts with the NSA, NGA, NRO, and DIA for "surveillance, reconnaissance, signals intelligence, and cyber warfare" (Shorrock, 2009). Recently Lockheed secured the "Geo-Scout" contract, a 10-year national program to connect all commercial and government satellites to a single network, the value of the contract is classified. In August 2008 the NGA awarded Lockheed with a \$32 million contract for managing communications networks during simulated war games (Shorrock, 2008)

Northrop Grumman is a contractor located in Falls Church, Virginia, that specializes in autonomous systems, cyber infrastructure, signals intelligence management and storage, systems engineering, and logistics (Northrup Grumman, 2016). Northrop employs about 22,000 people and has contracts with the DIA, NSA, CIA, and NGA. In 2005 Northrup secured a \$2-billion-dollar contract to modernize the information and technology infrastructure of Virginia (McDougall, 2005).

Raytheon also is headquartered in Falls Church, Virginia, and specializes in providing tools for "global intelligence, surveillance, and reconnaissance operations". Of the 9000 employees, 80% have top secret security clearance or higher. Raytheon has contracts with the NSA, NGA, and NRO for "signals and imaging processing, as well as information security software and tools" (Shorrock, 2008).

Through privatization programs, such as Operation Groundbreaker, intelligence contractors managed to transfer billions of dollars and thousands of jobs from the public sector to the private sector. Operation Groundbreaker was a \$5 billion contract to upgrade for the

telecommunications and computer networks at the NSA (Ellis, 2010). The NSA hired Booz Allen Hamilton and Northrup Grumman as consultants on the privatization operation. Companies that secured sub-contracts for services under Groundbreaker included: General Dynamics, BAE systems, Lockheed Martin, Northrup Grumman, and Verizon (Shorrock, 2008).

Now that the cyber-industrial complex has been identified, I will attempt to see if it has an effect on the policy formation process. The literature on iron triangles has identified a few key characteristics that are found in the CIC. The triangle features high barriers to policy process, few members involved in negotiations, and relatively stable positions of the members. My hypothesis stems from the flow of influence, legislation, and money, as they flow through the iron triangle. I hypothesize that the more money a Senator receives from intelligence contractors the more likely they are to vote in favor of surveillance activities.

Analysis

For my analysis I constructed two indexes to examine the effect of campaign contributions from private contractors on the voting behavior of senators. I used the data compiled by Open Secrets, a campaign finance website run by the Center for Responsive Politics (Center for Responsive Politics, 2016). I chose nine contractors that are major players in the cyber-industrial-complex: AT&T, Boeing, BAE systems, Booz Allen Hamilton, Boeing, General Dynamics, Lockheed Martin, Northrup Grumman, Raytheon and Verizon. I chose these companies because they are some of the largest intelligence contractors, they were all at least tangentially involved in the NSA's domestic surveillance programs, and they contribute significant amounts of money to the Senate. I selected seven roll call votes from the 114th Congress 1st Session of the United States Senate concerning surveillance and intelligence

gathering. I also included two variables that measured defense spending and defense personnel numbers by state, (Levinson, Shah, & Connor, 2011). These two variables will act as control variables and offer an alternative explanation as to why certain Senators may be receiving money from intelligence contractors.

Surveillance Index

The seven roll call votes are from three bills: H.R. 2048, S. 754, and S. 1357. Each of these bills relates directly to the surveillance vs privacy debate. H.R. 2048 was also known as the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act, or the USA FREEDOM Act. Originally a bill in the House to end the NSA mass surveillance programs, by the time it first reached the Senate in 2014, it was much different bill. As it went through the process of leaving the House Judiciary Committee and was passed by the house, it was slowly watered down with amendments. One clause that was removed during the amendment process would have required to the NSA to use “specific selection terms” in order to conduct surveillance on a target. This would have put an end to the bulk collection of internet and telephone programs outlined by the Snowden leaks. It failed to pass the Senate in 2014, because of the lack of real reform to the NSA surveillance activities.

The first action I collected data for was a cloture motion to proceed in May of 2015 that would have brought it to the Senate Floor for debate. The motion failed to pass 56-42, and was blocked from debate. For this motion I coded a “yes” vote as “0” and a “no” vote as “1” to create the variable Cloture_1. Those who wanted to reform the surveillance programs, and protect privacy would have voted for this motion, while those who did not want reform would have blocked. On June 2, the motion to proceed succeeded 77-17 and debate started.

The next three actions were all amendments offered by ex-officio SSCI member and Majority leader, Mitch McConnell in an attempt to keep the bulk collection programs intact. Amendment 1449 require that the SNI must certify that the USA FREEDOM ACT would not hinder national security or intelligence operations in any way, and also not require the release of the FISA court decision summaries. The secret court summaries would detail how and why certain targets were selected for surveillance. The amendment failed 43-56, for all three of the amendments I coded “yes” votes as “1” and “no” votes as “0”. Amendment 1450 would have delayed implementation of the USA FREEDOM one year if it was ultimately passed, it failed 44-54. Amendment 1451 would have removed the requirement that the FISA court provide written notice of when and why it chooses not to utilize the new *amicus curiae* oversight mechanism (Tien, 2015) , this amendment failed 42-56. Worth noting is how similar the vote totals are for each vote, and how they are divided almost directly down the partisan lines of 44 Democrats and 54 Republicans. I also recorded the totals from the final passage of the USA FREEDOM Act which passed 67-32. Ultimately the USA FREEDOM Act is seen as a victory for being able to end the government collection of bulk metadata, and have that information be held by the telecommunications companies. (Kelly, 2015) (Tien, 2015).

The next bill I examined was S. 1357, “a bill to extend authority relating to roving surveillance, access to business records and individual terrorists as agents of a foreign power under the Foreign Intelligence Surveillance Act of 1978 until July 31, 2015 and for other purposes. This bill was introduced by Mitch McConnell in an attempt to keep the surveillance programs completely intact, without any changes. For this bill I coded “yes” votes as “1” and “no” votes as “0”. The bill failed 54-45 (Senate.gov)

Finally, I tallied the vote for S. 754, also known as the Cybersecurity Information Sharing Act of 2015, it passed 74-21. As before I coded “yes” as “1” and “no” as zero. This bill would have offered immunity to companies that openly share information with the federal government, and was heavily opposed by pro-privacy groups like the Electronic Frontier Foundation, who claimed the bill would undermine privacy and that current cyber-security bills were sufficient (Jaycox, 2015).

Once I had the votes for each of the actions I was able to create an additive index that gave each senator a score from “0” to “7” that was indicative of their opinion regarding privacy and surveillance. A senator with a score of “0” would be strongly pro-privacy or anti-surveillance, whereas a senator with a score of “7” would be strongly pro-surveillance or anti-privacy. The mean on this index for the entire Senate was 3.27, almost directly in the middle of the scale. Senate Democrats had a much lower mean at .93, and Republicans had a much higher mean of 5.49. This difference of means highlights that surveillance is a highly polarizing issue that has very little middle ground. The independents, Bernie Sanders came in with a mean of 2.50.

Contributions Index

By combining the total contributions each candidate received from the above mentioned contractors, I constructed an index that would allow me get an idea of who was receiving money in the Senate. Only four members of the Senate did not receive contributions from these nine contractors, Cassidy, Ernst, Sullivan, and Tillis. Interestingly, out of those four only Sullivan comes in with a low score of “1”, while Cassidy, Ernst, and Sullivan scored “6”, “7”, and “7” indicating they are strongly pro-surveillance. The highest total was Republican Senator

Shelby from Alabama. For the Democrats the mean for the Contributions Index was \$103,337, the Republican mean was \$115,483, and the Independent mean was a much lower \$46,100. We can see here that on average the Republican Party receives more money on average than the Democrats and also has a higher score on the Surveillance Index, this gives me reason to examine this relationship further.

Party	Contributions Index	Surveillance Index
Democrat	\$103,337.44	.93
Independent	\$46,100	2.50
Republican	\$115,483.70	5.49
Total	\$108,630.21	3.27

For the next step of my analysis I decided to see the strength of the relationships between my variables by performing a correlation.

	Surveillance Index	Contributions Index	Defense Spend	Personnel
Surveillance Index	1	R=.220* Sig=.034	R=-.041 Sig=.695	R=.074 Sig=.480
Contributions Index	R=.2208 Sig= .034	1	R=.171 Sig=.089	R=.192 Sig=.056
Defense Spend	R=-.041 Sig=.695	R=.171 Sig=.089	1	R=.783** Sig=.000
Personnel	R=.074 Sig=.074	R=.192 Sig=.056	R=.783** Sig=.000	1

Correlation is Significant at the 0.05 level-*

Correlation is Significant at the 0.01 level-**

My variables did not correlate strongly enough to prove a strong relationship, but my Surveillance Index and Contribution Index have a significant correlation at the .05 level which

does support my hypothesis. There are a few relationships that correlate very strongly such as personnel and defense spending, which makes sense since greater spending is needed for greater numbers of personnel. This creates a concern of collinearity, which is when two variables that have high correlation are used in a regression equation. So far Party identification has the strongest correlation with the Surveillance Index with a very high R of .793 and a very low p of .000.

For the next part of my analysis I ran a regression including all of variables with the formula:

$$\text{Surveillance Index} = Y = (\text{Party}) + (\text{Contributions Index}) + (\text{Defense Spend}) + (\text{Personnel})$$

	B	Std. Error	Beta	t-score	Sig
(Constant)	.303	.381		.795	.429
Party_dum	4.516	.376	.128	12.007	.000
Index of Contributions	4.209E-6	.000	.017	1.946	.055
Defense Spend	5.928E-12	.000	.049	.179	.858
Personnel	2.822E-6	.000	.786	.510	.612

r=.637

After doing this first regression I can see that the relationship with strongest explanatory power for the value of the Surveillance Index, is Party identification, with a $t > 2$ and a $p < .05$. My correlation gave me reason to reject the null hypothesis and think that there might be relationship between the Surveillance Index and the Contributions index, with the $p < .05$ and $r=.220$. Once the other variables are included to offer an alternative explanation for the change, the strength of the relationship decreased and produced a $t < 2$ and a $p > .05$. While the Contributions Index does have an effect on the Surveillance Index, the relationship is not strong

enough to be significant. In order to investigate further, as well as try to control collinearity, another regression needs to be performed.

This time certain variables were recoded in order to make the final output more legible. Since the total amounts for the variables personnel, Contributions index, and defense spending were such large numbers, they appear in the regression in scientific notation. To control this, personnel and contributions index were reduced to display their values in thousands, instead of the whole number. Defense spending was also reduced to display their value in billions of dollars. For example, the value of 56,000 personnel was recoded to be 56.0, \$125,000 in contributions was recoded to read 125.0, \$42,100,000,000 was recoded to 42.10. This resulted in making the regression much easier to read. In order to control for collinearity with the variables defense spending and personnel, each were excluded from one regression to see doing so would have an effect on the t-score, p-score, and R square.

The formula for the second regression was:

$$\text{Surveillance Index} = Y = (\text{Party}) + (\text{Contributions Index per 1000}) + (\text{Personnel per 1000})$$

	B	Std Error	Beta	t-score	Sig
Constant	.321	.364		.881	.381
Contributions per 1000	.004	.002	.129	1.978	.051
Party	4.501	.365	.783	12.334	.000
Personnel by 1000	.004	.004	.061	.946	.347

r=.641

As we can see, recoding the variables to decimals succeeded in making the output readable without scientific notation. Also, r increased from .637 to .641, while this is not a

major increase it does show that removing the variable for defense spending did change the results of the regression. Most notably, the t-score for the contributions index also increased from 1.946 to 1.978, nearly to the $t > 2$ standard needed for a sound regression. The p-score also decreased from .055 to .051, also approaching the standard needed, $p < .05$. The standardized coefficients, or Beta, can be interpreted like the Pearson coefficient, 0 meaning no correlation and 1 being perfectly correlated. Party identification still correlates most strongly with the surveillance index at .783, but a value of .129 shows there is a relationship there. Another regression is needed, and this time personnel will be substituted for defense spending in order to see if more predictive power can be found. The formula for the final regression will be:

$$\text{Surveillance Index} = Y = (\text{Party}) + (\text{Contributions per 1000}) + (\text{Defense per billions})$$

	B	Std. Error	Beta	T-score	Sig.
Constant	.313	.378		.826	.411
Contributions per 1000	.004	.002	.131	2.011	.047
Party	4.541	.371	.790	12.225	.000
Defense Spending in Billions	.018	.022	.054	.815	.418

$r = .640$

In this regression, the adjusted r-squared actually decreased from .641 to .640, this shows that switching personnel and defense spending did have an effect on the regression. The t-score for contributions index is now greater than two and the p-score is significant at the .05 level, meaning the null hypothesis that contributions index has no effect on surveillance index can be rejected. Beta also increased from .129 to .131, which shows an increase in correlation between the two variables. B is responsible for showing the extent of change expressed in Y for

every unit increase in X. In this case, for every \$1000 in campaign contributions a Senator receives, the value of Y increases by a value of .004, meaning the move closer towards being pro-surveillance. While this doesn't sound like very much, we must keep in mind that some of the Senators in question receive hundreds of thousands of dollars from intelligence contractors.

Conclusions

At first, my analysis suggested that the null hypothesis that contributions have no effect on their score for the surveillance index should be accepted. However, after reworking the regressions to control for collinearity, a $t > 2$ and a $p < .05$ was achieved. While party identification still possesses much stronger predictive power for the surveillance index, the contributions index has been proven to have a statistically significant effect. This effect is not exceptionally strong but it does support my original hypothesis that Senators who receive money from intelligence contractors will be more likely support surveillance activities. In the future, I would like to expand this dataset to include the House of Representatives. I believe that since there are a much greater number of Representatives than Senators, this phenomenon could be better examined.

In addition to the quantitative research, I have also shown through my qualitative research that there is a cyber-industrial complex similar to the military-industrial complex. The IC policy community has characteristics of both Iron Triangles while in secret, and Issue Networks once exposed. That it has a well-established network of both formal and informal relationships that insulate it from outside pressures, so long as it stays a secret. As long as the IC can hide behind a veil of secrecy, we may never really know the full extent that the cyber-industrial complex has on the policy making process.

Works Cited

- Center for Responsive Politics. (2016). *Politicians and Elections*. Retrieved from Open Secrets: www.opensecrets.org/elections/
- Eisenhower, D. D. (1961, January 17). *Farewell Address to the Nation*. Retrieved December 4, 2015, from Eisenhower Presidential Library : eisenhower.archives.gov
- Electronic Frontier Foundation. (2013). *How the NSA's Domestic Spying Program Works*. Retrieved from Electronic Frontier Foundation: <https://www.eff.org/nsa-spying/how-it-works>
- Ellis, W. W. (2010). Us Intelligence at the Crossroads. *Mediterranean Quarterly*, 21(2), 1-11.
- Erwin, C. (2013). NSA Surveillance Leaks: Background and Issues for Congress. *Current Politics and Economics of the US, Canada, Mexico*, 15(2), 139-159.
- Fang, L. (2015, 4 9). *Lobbyists for Spies Appointed to Oversee Spying*. Retrieved from The Intercept: www.theintercept.com/2015/04/09/lobbyists-for-spies-appointed-to-oversee-spying
- Federal Judicial Center. (n.d.). *History of the Foreign Intelligence Surveillance Court*. Retrieved from Federal Judicial Center: [Fjc.gov](http://fjc.gov)
- Gais, P. W. (1984, April). Interest Groups, Iron Triangles and Representative Institutions in American National Government. *British Journal of Political Science*, 14(2), 161-185.
- Ginsberg, L. W. (2013). *We The People*. New York: W.W. Norton Company.
- Goldman, R. (2013, June 10). *The Secret History of NSA Contractors*. Retrieved from ABC News.
- Greenwald, G. (2014). *No Place To Hide*. New York, NY: Henry Holt and Company.
- Greenwald, G., & MacAskill, E. (2013, June 11). *Boundless Informant: the NSA's secret tool to track global surveillance data*. Retrieved from The Guardian: <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>
- Halchin, E. (2015). *The Intelligence Community and its Use of Contractors: Congressional Oversight Issues*. Congressional Research Service. District of Columbia: Federation of American Scientists.
- Hecl, H. (1978). Issue Networks and the Executive Establishment. In A. K. Samuel Beer, *The New American Political System*. District of Columbia: American Enterprise Institute for Public Policy.
- Jerry Brito, T. W. (2011). Loving the Cyber Bomb? The Dangers of Threat Inflation in Cyber Security Policy. *Harvard National Security Journal*, 3.
- John Foster, R. M. (2014, Aug). Surveillance Capitalism: Monopoly, Finance Capital, the Military Industrial Complex, and the Digital Age. *Monthly Review*, 66(3), 1-31.
- Jordan, A. G. (1981). Iron Triangles, Woolly Corporatism, and Elastic Net: Images of Policy Process. *Journal of Public Policy*, 95-123.
- Kelly, E. (2015, June 2). *Senate Approves USA Freedom Act*. Retrieved from USA Today: <http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/>
- Landau, S. (2013, August). Making Sense from Snowden. *IEEE Security and Privacy*, 56-62.
- Levinson, R., Shah, S., & Connor, P. (2011). *Impact of Defense Spending in State-by-State Analysis*. Bloomberg Government. Bloomberg L.P.

- Liu, E. (2014). Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments. *Current politics of Economics in the United States, Canada, Mexico*, 69-81.
- Markusen, A. R. (2003, October). The Case Against Privatizing National Security. *Governance: An International Journal of Policy, Administration, and Institutions*, 16(4), 471-501.
- McDougall, P. (2005, 11 15). *Virginia Taps Northrop Grumman for \$2 Billion IT Overhaul*. Retrieved from informationweek.com: [http://www.informationweek.com/virginia-taps-northrop-grumman-for-\\$2-billion-it-overhaul/d/d-id/1037969?](http://www.informationweek.com/virginia-taps-northrop-grumman-for-$2-billion-it-overhaul/d/d-id/1037969?)
- Northrop Grumman. (2016). *About Northrop Grumman*. Retrieved from NorthropGrumman.com: <http://www.northropgrumman.com/aboutus/Pages/default.aspx>
- Peterson, A. (2013, December 31). *Here's what we learned about the NSA's spying programs in 2013*. Retrieved from The Washington Post: <https://www.washingtonpost.com/news/the-switch/wp/2013/12/31/heres-what-we-learned-about-the-nsas-spying-programs-in-2013/>
- Ray, M. (2015, 10 22). *Edward Snowden*. Retrieved from Encyclopedia Britannica: britannica.com
- Shorrock, T. (2008). *Spies for Hire: The Secret World of Intelligence Outsourcing* (Vol. 1). New York, NY: Simon and Schuster Inc.
- Shorrock, T. (2009, November 16). *Spies for Hire: Who's Who in Intelligence Contractors*. New York: spiesforhire.org.
- The Editors of Encyclopedia Britannica. (2015, 7 3). *National Security Agency*. Retrieved from Encyclopedia Britannica: britannica.com
- The Washington Post. (2011). *Companies*. Retrieved from Top Secret America.
- Thomas Gais, M. P. (1984). Interest Groups, Iron Triangles, and Representative Institutions. *British Journal of Political Science*, 14(2), 161-185.
- Tien, L. (2015, June 2). *EFF Opposes Amendments that Weaken USA Freedom Act*. Retrieved from Electronic Frontier Foundation: <https://www.eff.org/deeplinks/2015/06/eff-opposes-amendments-weakening-usa-freedom-act>
- U.S. Senate Select Committee on Intelligence. (2016). *About the Committee*. Retrieved from U.S. Senate Select Committee on Intelligence: www.intelligence.senate.gov/about
- Yoo, J. (2014). The Legality of the National Security Agency's Bulk Data Surveillance Programs. *Harvard Journal of Law and Public Policy*, 901-930.