THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF ECONOMICS

NATIONAL INTELLIGENCE: AN ECONOMIC PERSPECTIVE

MARK RYAN
SPRING 2016

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees
in Economics and Security and Risk Analysis
with honors in Economics

Reviewed and approved* by the following:

Colin Knapp
Senior Lecturer of Economics
Thesis Supervisor

Russell Chuderewicz
Professor of Economics
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

Since 9/11, the U.S. Intelligence Community has been scrutinized and evaluated for their effectiveness and efficiency in preventing terror attacks and combating foreign threats to national security. Several mistakes and poor intelligence conclusions have led to several reforms and scrutinization of the entire intelligence process. This paper will look at the national intelligence from an economic perspective and use economic techniques to model the market for intelligence. Because of the classified nature of the intelligence process and the lack of transparency between the taxpayer and government, there are many information issues that impede the market for intelligence from reaching equilibrium. This paper will help model this market, and its current inefficiencies, while proposing policies to help increase the likelihood of reaching equilibrium in the future.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

First, I would like to thank Professor Colin Knapp of the Pennsylvania State University for his time, advice, expertise and support as I worked through this paper. I would like to acknowledge the Economics Department at Penn State for giving me the skills I need in order to have written a successful thesis. Finally, I would like to thank all my friends and family who have supported me throughout my undergraduate education.

Introduction

The September 11th, 2001 terror attacks on U.S. soil would forever change the way the U.S. combats international threats. The rise of terrorism brought about a new challenge for the U.S. Intelligence Community (IC). Because the threat landscape changed for the IC, the structure of the intelligence process also underwent changes. However, this country has seen several intelligence failures since 9/11. This includes a 2003 intelligence report that Iraq had weapons of mass destruction, resulting in military action, which was later discredited. In the past 6 years, the U.S. IC has seen several disclosure events of classified information, leading to more scrutiny and review of IC processes.

The intelligence failures indicate an economic market failure. Few have looked at national intelligence as an economic good, or from an economic perspective. This paper does just that. When describing intelligence from an economic perspective, the issues in the market for intelligence come to light, and allow the possibility of finding policies to reduce the likelihood of a future intelligence failure. First, this paper will describe the intelligence good and intelligence process in the U.S. Then, literature review will frame intelligence as a public good. Externality and risk analysis frameworks will help depict issues with the current intelligence process, and principal-agent theory will describe the issues with the relationship between the taxpayer and the U.S. government. It is important to investigate intelligence from an economic perspective in order to promote efficiency equilibrium in the intelligence market to avoid more failures in the future.

Chapter 1: U.S. Intelligence Landscape

Before understanding how to look at intelligence gathering from an economic perspective, it is important to have a basic understanding of the logistics of how intelligence is gathered in the United States. Intelligence is a term that can represent a process, the methods by which information is collected, and a product, the actual information gathered that gives insight on the capabilities and intentions of adversaries. Intelligence will be used interchangeably between these two definitions to describe the environment in which decisions are made, but the economic analysis will strictly refer to the intelligence as an economic good. As a good, intelligence can be broken into the production side, facilitated by the various groups outlined below, and consumption by the taxpayer and those under the protections of the U.S. Government. The following section is intended to introduce the intelligence gathering process in the United States, and look into detail on how the intelligence gathering process is funded.

Types of Intelligence

While the majority of this analysis will group intelligence as one homogeneous good, it is important to understand that there are different types of intelligence that play different roles in the IC. Each has different costs and benefits associated with it. This section will briefly describe the types of intelligence to provide context for later analysis of the costs and benefits of intelligence collection.

Many stereotypes about the IC include the image of spies and James Bond-like activities. This type of intelligence gathered by human agents is called Human Intelligence (HUMINT). HUMINT can be covert or overt (Lowenthal, 2015, p46). Information gathered from HUMINT

can include details about enemy weapons systems, research, or even information about the social or economic plans of a country. HUMINT requires a robust network of human agents and sources. (Richelson, 2012 p293)

This type of intelligence has gained more media attention through the news recently from the 2013 National Security Agency leaks incident. Signals Intelligence (SIGINT), at its core, is the collection of intelligence from intercepting signals of communications (Lowenthal, 2015, p46). The interception of communications can provide a variety of information about targets. SIGINT can vary from intercepted diplomatic communications of large nations to the chatter produced on terrorist network channels (Richelson, 2012 p204-205). It requires a vast infrastructure of satellites and other communications interception technologies that are expensive to produce.

Other types of intelligence, while not as prominent as HUMINT or SIGINT, are associated with intelligence collection. Geospatial Intelligence (GEOINT) and Imagery Itelligence (IMINT) refer to intelligence gathered from photographic or satellite imagery analysis (Lowenthal, 2015, p46). Measures and Signatures Intelligence (MASINT) is a relatively new type of intelligence, which involves looking at specific characteristics of events and objects to try to identify hidden operations. This includes radar analysis, nuclear radiation analysis and materials analysis. (Richelson, 2012 p240). It is clear that the term intelligence does not refer to a homogeneous process of gathering information, rather it includes a wide variety of disciplines that require an array of resources that have numerous, diverse benefits.

Targets/Threats

Understanding the types of threats mitigated by intelligence collection gives insight on just what benefits intelligence gathering provides. Jeffrey Richelson argues that the IC has three distinct types of targets: transnational targets, regional targets, and national targets (Richelson, 2012, p7-9).

Transnational targets refer to threats that extend past any single country's borders and have the ability to affect all corners of the world. These threats include terrorist groups and cyber terrorism. Terror groups have become more of a threat over the last decade with the increase of popularity of asymmetric warfare. In recent years, there have been terror attacks in many major cities across the globe, and many transnational terror groups claiming responsibility for these attacks. Richelson notes these type of threats require a different set of tactics to combat than typical national threats as they act and operate less centrally. By definition, a cyber threat is not associated with any geographical boundaries and has the potential to have a far-reaching, negative effect on the United States. Regional threats refer to the idea that there are threats not just associated with one specific government, but are a result of friction between neighboring governments. One example of this is the Middle East and the threat posed by the regional instability. Finally, Richelson describes national threats as country/government actors that the IC collects intelligence on. One important note that Richelson makes is that these threats can be from friendly as well as unfriendly countries. The rise of the Chinese and the nationalist sentiments of Russia make both national threats. Richelson states that national threats require the most resources, as they are associated with the largest threats (Richelson 2012, p7-9).

Hierarchy of the Intelligence Community

The U.S. IC is very hierarchical. The President of the United States oversees all intelligence activities and has the final word on agenda setting for any agency or group collecting intelligence on behalf of the government. Much of the agenda setting and priority making falls to the National Security Council (NSC). The NSC is comprised of the President, Vice President, Secretaries of State, Defense, and Treasury, as well as other senior intelligence officials (The White House). After 9/11, the Bush Administration and Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) which created the position of the Director of National Intelligence (DNI) (Lowenthal, 2015, p37). This position was created to have an advisor to the NSC and the president, and to have someone working directly with the heads of every intelligence agency except the Central Intelligence Agency (CIA). The Director of the CIA reports directly to the NSC, not to the office of the DNI (ODNI). The DNI is responsible for all intelligence activities in the U.S. and works to ensure every agency is sharing their information effectively (Lowenthal, 2015, p38). The ODNI is comprised of the DNI and intelligence officials from major intelligence agencies (Lowenthal, 2015, p41).

The CIA is unique among the intelligence agencies as it's director has a more powerful role and reports directly to the President and NSC rather than the ODNI. Before 9/11, the DNI didn't exist and, the Director of the CIA held many responsibilities that the current DNI has. A consequence from the past is that the CIA does not fall under a smaller umbrella hierarchically in the intelligence structure. The CIA has been in existence since the 1940s and is considered an all-source collection agency meaning it collects many different types of intelligence (Lowenthal, 2015, p91-92). For budgetary reason, it is considered a civilian agency.

While the CIA doesn't fall under any other branch of intelligence, the National Security Agency (NSA), National Geospatial Agency (NGA), the National Reconnaissance Office (NRO) and the Defense Intelligence Agency (DIA) all fall under the umbrella of the Department of

Defense (DoD). The Secretary of Defense plays a large role running these agencies and setting intelligence priorities. Like the CIA, the DIA is an all-source intelligence collection agency within the Department of Defense and plays a large role in the creation of intelligence products. The NSA has two main missions: collecting SIGINT and providing information assurance which involves protection of critical U.S. communication and information systems (Richelson, 2012 p32). The NGA is the leading agency on geospatial intelligence and imagery intelligence. While the charter of the NGA includes many responsibilities, their primary goal is to provide GEOINT and IMINT products to support the Department of Defense mission (Richelson, 2012 p44). The NRO is an anomaly in two ways. First, other agencies and military arms appoint employees to work for the NRO. Second, the NRO is not a pure intelligence agency as its mission space does not include creating intelligence as a product. The NRO is essentially the research and development arm of the Department of Defense intelligence mission (Richelson, 2012 p35-41).

Each branch of the U.S. military plays a role in collecting and producing intelligence as well. Military intelligence structures tend to be more insulated from their civilian agency counterparts and are more focused on gathering intelligence that supports their own operations. The separation of military and civilian structures leads to a common criticism that intelligence groups tend to duplicate their efforts (Richelson, 2012 p79-80). Although military intelligence tends to be for the short-term needs, it is critical in the protection of U.S. assets.

The Federal Bureau of Investigation (FBI) and the Drug Enforcement Agency (DEA) both play a role within the intelligence community under the authority of the of the U.S. Attorney General. While the main mission space of these agencies is primarily law enforcement, both produce intelligence that contributes to the mission of the IC. For example, the FBI plays a role in domestic counterterrorism (combating terrorist actions) and counterintelligence

(combating the actions of other intelligence agencies) efforts, thwarting attacks on U.S. soil unlike the other agencies described (Richelson, 2012 150). The focus of the FBI and DEA are domestic only.

The Secretary of Homeland Security is in direct control of the Department of Homeland Security (DHS) and the Coast Guard (Lowenthal, 2015, p41). The Department of Homeland Security is actually a collection of twenty-two different agencies including U.S. Customs Service, the Secret Service, Federal Emergency Management Agency, and many more. The primary role of DHS is to protect domestic assets and was created in direct response to the 9/11 attacks. From an intelligence perspective, DHS has a mission to not only prevent terror attacks from transnational threats, but to also collect intelligence to protect critical infrastructure, provide border security, and identify and mitigate cyber threats. The broad mission space of DHS contributes to the wellbeing of taxpayers that fund DHS and all of its agencies.

Intelligence Budgets

Perhaps the most important piece of the intelligence landscape for the economic perspective is how intelligence is funded. As will be discussed later, intelligence products are a public good and thus are funded by taxpayers. The budget for the intelligence community is actually split into two budgets: the National Intelligence Program (NIP), and the Military Intelligence Program (MIP). The NIP is larger and includes funding that transcends single agencies or are nondefense in nature (Lowenthal, 2015, p63). The MIP is mostly for military and defense agencies. Most organizations receive money from only one of the budgets, but the NSA and NGA receive funding from both sources (Lowenthal, 2015, p67). In fiscal year (FY) 2015,

the total federal intelligence budget was $66.8 billion with $16.5 billion slated for the MIP and $50.3 billion portioned for the NIP (Federation of American Students, 2016). For comparison's sake, the total federal budget for FY15 was $3.69 trillion, about $590 billion was budgeted for national defense, where the NIP and MIP are located (Office of Management and Budget, 2016). The DNI distributes the money from the NIP and funds the CIA, FBI, NRO, and programs within the NSA, NGA, Department of the Treasury, Department of Homeland Security, Department of Energy, and the DIA (Lowenthal, 2015, p67). The intelligence budget peaked in 2010 at just over $80 billion and has decreased every year since (Federation of American Students).

Appendix B contains a table that shows the rise and fall of the NIP and MIP over the past decade and how spending varies with needs and priorities of the country. If the appropriated amounts for each budget are close to the requested amounts for FY2016, we will see the first increase in the intelligence budget since 2010. While the NIP and MIP are regarded as the key budgets that fund the intelligence community, there are yearly expenditures that contribute to the production of intelligence products. For example, in FY17 the Department of Homeland Security is slated to receive $47.75 billion (1.15 percent of the total FY17 budget) outside of their usual NIP funding (Office of Management and Budget, 2016) which includes money for defense-related activities and efforts to protect against violent extremist attacks (Office of Management and Budget, 2016).

If spending for the MIP and the NIP is approved, the pure intelligence budget will amount to $70.3 billion of the total $4.15 trillion budget, and the $1.23 trillion portioned for discretionary spending (Office of Management and Budget, 2016). While this is under 2 percent of the total budget, it still comprises a substantial portion of the total spending, coming in at

about twice the amount we spend on highways and infrastructure, and about six to seven times the total expected budget of the U.S. Coast Guard. It's clear that the budget for the IC is large enough to make up a substantial piece of the overall budget and thus costs taxpayers a significant amount of money each year.

Intelligence Oversight

The Foreign Intelligence Surveillance Court (FISC) was established in 1978 when Congress passed the Foreign Intelligence Surveillance Act. The court is located in Washington D.C, and is made up of eleven appointed federal judges (Foreign Intelligence Surveillance Court). Much of the court is closed due to the classification of the material involved in court proceedings, but has the authority to approve the investigative methods of the IC including "(1) electronic surveillance; (2) physical searches; (3) pen registers/trap and trace surveillance and (4) orders to compel the production of tangible things" (Cole, 2014, p2). In addition, this court has jurisdiction over issues regarding the targeting of non-U.S. persons abroad (Cole, 2014, p2). Because of the secret nature of this court, it is difficult to even estimate the costs of this court on the taxpayer, but the entire FISC wouldn't be necessary or exist without the creation of the intelligence process, thus costs of producing intelligence must clearly include the costs of running this court.

In addition to costs on the judicial branch, the intelligence production process imposes costs on the legislative branch as well. Both chambers of Congress have a designated committee for intelligence oversight. The House of Representatives Permanent Select Committee on

Intelligence (HPSCI) is comprised of 22 members of the House of Representatives and is made of subcommittees focused on the CIA, Department of Defense, emerging threats, and the NSA and Cybersecurity (The Permanent Select Committee on Intelligence). The HPSCI has jurisdiction over the agencies that make up the NIP and the MIP (Belfer Center for Science and International Affairs, 2009). The Senate Select Committee on Intelligence (SSCI) is smaller, made up of 13 U.S. Senators (SSCI) and has jurisdiction over the members of the NIP, but not the MIP (Belfer Center for Science and International Affairs, 2009). In addition to the HPSCI and the SSCI, the House and Senate armed services committees share oversight functions of military intelligence programs.

Congress plays several key oversight roles over the intelligence community. First, Congress has the ability to authorize and appropriate funds for specific intelligence-related programs. Ultimately, Congress has the ability to defund and eliminate entire programs, and create new funds for other programs based on the priorities of. This is a powerful tool Congress has over the IC. Second, the Senate has the power to approve presidential nominations for heads of agencies and departments important to the IC. Not only can the Senate disapprove of nominations that are not aligned with the Senate's own goals and priorities, they can threaten to withhold a nomination until changes within the IC are made or the IC makes some sort of concession to the will of the Senate (Belfer Center for Science and International Affairs, 2009). Finally, Congress is able to hold hearing and conduct investigations into the activities of the IC (Center for Science and International Affairs, 2009). After the 2013 NSA leaks incident, we saw investigations and hearings about the alleged activities of the NSA that were used as a tool to increase public pressure on the IC and produce changes.

Between the judicial and legislative branches and their oversight roles for intelligence production, there is a clear cost to other government institutions to produce intelligence that is not captured in the budgets for the NIP and the MIP. While it is outside of the scope of this paper to calculate the exact costs on other government institutions brought about by intelligence gathering, it is simply important to understand from an economic perspective that the cost of collecting intelligence is not simply the dollar amount allocated to intelligence activities. Taxpayers fund Congress and the FISC, thus the costs associated with intelligence oversight are passed on to the taxpayers/consumers of intelligence. From this, we can see that consumers are not just consuming intelligence products, but the entire intelligence process including oversight costs.

Chapter 2: Intelligence as a Public Good

Intelligence, much like national defense, has a strong public good aspect associated with it and this section seeks to describe intelligence as a public good in terms of several different models of public goods.

Samuelson

Paul Samuelson presents a model where he separates all goods into two types: private goods and collective consumption goods. A private good is finite and one person's consumption of the good takes away from another individual's ability to consume the good. Collective consumption goods exist where everyone can consume a good without affecting another's utility level. In his model, goods that are private and are under a condition of perfect competition do not need any government intervention to reach a social optimum. His model claims goods will be produced and consumed at the lowest cost leading to a socially efficient outcome. A key point Samuelson makes is that "no decentralized pricing system can serve to determine optimally these levels of collective consumption" (Samuelson, 1954 p388). Therefore, he concludes that the collective consumption goods need government intervention in order to achieve the social optimum and that the marginal cost of production must equal the marginal benefit of consumption, know as the Samuelson condition.

By Samuelson's basic definition, national intelligence is certainly a collective consumption good. The producers of national intelligence, almost exclusively federal

government agencies, produce intelligence to benefit all citizens of the United States. One person's consumption of intelligence does not affect the consumption of another person. This implies that the socially optimum quantity of intelligence would not be produced in a decentralized manner. Without the presence of the government in the collection and production of intelligence, it is very unlikely that national intelligence would be collected at all. The benefits of national intelligence have the potential to affect every citizen of the United States, but the costs of producing intelligence are too high for any private firm to enter the market. We will see with other models of public goods that there are many issues preventing a private, competitive market environment for national intelligence, but with regard to Samuelson's model, national intelligence can certainly be described as a collective consumption good.

Oakland

Oakland provides a thorough analysis and theory of public goods and his own theory of public goods that can be used to analyze intelligence from a public good perspective. Oakland's theory provides several key qualifiers in the definition of a public good that were not included in Samuelson's original work. One of these key ideas is that public goods must "be of interest to more than one consumer or firm" (Oakland, 1987 p485). He argues that if only one person is interested in consuming the good, or producing it, then the condition of one person's consumption not being affected by another's would be irrelevant. Oakland uses an example of how a firework display in an empty desert would be considered a private good, but the same display in a park with people would be considered a public good (Oakland 1987, p485). In the

case of national intelligence, this condition is met, although it brings about a potential complication not presented in Oakland's analysis: blind consumption.

The means by which intelligence is collected in the United States and the classified nature of much of the information collected by intelligence agencies leads to a phenomenon where consumers of intelligence don't actually know what they are consuming. Intelligence is collected behind a shield of secrecy from those who enjoy the utility from the good. Consumers are not aware of how much intelligence they "consume" or, more importantly, the level of utility that intelligence collecting gives to consumers. This leads to the notion of blind utility.

The ideas of blind consumption and blind utility do not inhibit the treatment of intelligence as a public good. The assumption that consumption of the good by one person does not affect the consumption of another is not affected with the introduction of blind consumption (Samuelson definition). Therefore, Samuelson's definition still holds. It just means many people must consume intelligence blindly at the same time which is certainly the case since all citizens of the U.S. consume the good and receive some benefit from intelligence collecting.

Oakland's analysis of public goods deals with what he describes as a pure public good. A pure public good is one in which the producers of the good cannot exclude anyone from consuming their good without incurring some type of cost. Oakland points out the problem with such a good in which the marginal cost of another consumer is zero and there is no possibility of costless exclusion: how to achieve an efficient outcome in which the Samuelson condition is realized. In this case, Oakland argues that there needs to be a policy solution in order to reach an efficient outcome in which a pure public good is funded (Oakland, 1987 p490).

In the case of intelligence gathering, the policy solution is tax funding. The government agencies that collect intelligence benefitting everyone in the United States are federally funded.

The Department of Defense budget is over $500 billion (National Defense Budget Estimate FY15), funded by the tax dollars of U.S. citizens, and much of this budget goes toward intelligence gathering. Without taxing, there would be no intelligence agencies to gather intelligence. The policy solution that Oakland describes as needed in order to attempt to produce an efficient outcome is represented in the tax funded budgets Congress passes for intelligence agencies to use. The fact that intelligence gathering benefits everyone in the United States with no marginal cost of another person consuming the intelligence, and that there need be a policy solution, taxation, in order to ensure the efficient amount of intelligence is produced is evidence to support the argument that national intelligence is indeed a public good. Whether or not the efficient level of intelligence is being produced, and the level of tax spent on intelligence gathering is efficient will be discussed later in this paper, but Oakland's analysis helps put national intelligence in the frame of a public good.

Another aspect of a pure public good as described by Oakland is that the good benefits all consumers equally (Oakland, 1987 p492). This facet of a public good is not necessarily seen in intelligence gathering. Although all U.S. citizens benefit from intelligence, they do not benefit equally. That is, each citizen of the United States consumes and benefits from intelligence if the intelligence helps improve their utility. The benefits of intelligence gathering are not equal among all consumers because the utility provided by intelligence comes in the form of increased life expectancy, and the chances of a terror attack are not equal for all citizens of the U.S.

Terror attacks are more successful, in the eyes of the terrorists, if the attack produces shock and awe and gains a great amount of media coverage. An attack on a small, rural would not have nearly the power that an attack on a major metropolitan area would have. This creates a differential impact across consumers based on location. The intended attack locations of the 9/11

hijackers support this claim; each target was an important government/economic landmark where a lot of people were located in order to produce fear and gain media coverage. With this logic, we can assume that consumers of intelligence are of unequal chance of being harmed by a terrorist attack and thus are not benefitting equally from intelligence that prevents terrorist attacks. The direct benefit of a piece of intelligence that prevents a terrorist attack is only given to those who would've been negatively affected by the attack.

A key point to acknowledge here that will be important later in this paper is that that chance of terrorist attack on any citizen of the U.S. is assumed to be non-zero. That is, there is no consumer of national intelligence and no person taxed to fund national intelligence that receives zero benefit from intelligence gathering. While the chances of an attack could be argued to be significantly lower for some U.S. citizens than others, it will be assumed that there is always a chance of an individual being negatively affected by a terrorist attack in his/her lifetime. The rationale behind this assumption could be that almost everyone travels at some point in their lifetime toward a metropolitan area, and/or terrorist capabilities/intentions could include attacks that affect a wide area of attack. Without this assumption, the possibility exists that people could move to geographic locations, or take other actions to eliminate the need for intelligence gathering and that a private market for preventing terrorist attacks could exist outside of intelligence gathering.

Oakland proves that the Samuelson condition, that marginal benefit must equal marginal cost for an efficient outcome, is still true even if the distribution of utility gained from the good is not uniform. In his analysis, Oakland creates a good that provides some negative utility to some and positive utility to others. Here, he proves that the Samuelson condition holds if the total utility gained from the public good is positive. That is, if the sum of the magnitude of the

positive utilities is higher than the absolute value of the sum of the magnitude of negative utilities, then there is still the possibility of an efficient market where the marginal cost of production equals the marginal benefit to society. While the benefits to consumers of intelligence is higher to some than others, utility from intelligence gathering is assumed non-zero and positive for each person in the United States thus the net benefits of intelligence gathering to its consumers will always be positive and the Samuelson condition will hold true.

While national intelligence is not a pure public good by Oakland's definition, the good can still be analyzed from a public good perspective. National intelligence is of interest to more than one producer or consumer, producers of intelligence cannot, without cost, exclude people in the U.S. from consuming the good, and the net utility of producing intelligence is positive.

Chapter 3: Externalities

In his book, *The Economics of Welfare,* Arthur Pigou describes the concept of externalities. He explains how some goods can have costs or benefits that are given to people who are not the direct consumers or producers of the good. These spillovers produce either a negative or positive externality depending on the nature of the effect. If a factory moves into a town, it could have a negative impact on people in the surrounding area with spillovers such as pollution and congestion. A free market does not force the firm to internalize these costs and the firm will produce too much of the good from society's point of view. Pigou suggests that government intervention is needed to overcome this issue and that government could tax the good to internalize the externality. If the tax is equal to the external costs, society will produce the socially efficient amount of good. Alternatively, spillover effects could be positive in which case Pigou says that the government could subsidize the good to lower costs and increase the quantity of the good produced (Pigou, 1920).

Pigou's concept of externalities is very relevant to intelligence collection. Intelligence collection is a good that has a wide variety of far reaching effects, both positive and negative. A notable caveat to make here is that the likelihood of someone being harmed in a terrorist attack in the United States on any given day is negligible, with only 17 U.S. citizen deaths attributed to terrorism in 2011. (U.S. Department of State, 2011). Since 2000, there have been 209 "incidents" of terrorism in the United States alone, many of which did not result in any deaths or injuries. In comparison, the same statistic from a country with greater levels of terrorism, such as Afghanistan, is much higher at 7,641 (University of Maryland, 2015). From this, we can infer that the expected benefit of intelligence collection is rather low considering the risk of being involved in a terror attack is almost zero per person. These numbers are not completely

representative of the relative need for intelligence gathering because it does not take into account the number of terror attacks, and thus the saved potential losses resulting from intelligence gathering. The United States government does not publish information about the number of prevented terror attacks that intelligence gathering has prevented, nor the economic value of these prevented attacks. One of the closest indicators we have is after the 2013 leaks of NSA actions, the head of the NSA testified before congress stating that the program prevented 54 terrorist attacks in the six years it was active. After investigation, the NSA was forced to redact that statement after is was found that only 13 of the 54 attacks would have affected Americans, and not all of these 13 were confirmed planned attacks (Waterman, 2013). This illustration shows that the records of prevented terrorist attacks, and thus the benefits of intelligence gathering, are mostly not available and subjective. Therefore, this following section will focus on the examination of the types of benefits and costs associated with intelligence collection, and the components of supply and demand, rather than attempting to calculate exact costs and benefits of intelligence gathering per capita with incomplete, and inconsistent information.

Private Benefits

As with many goods, there is a private benefit to intelligence gathering. This accrues to the group or individual doing the intelligence collection. There are many parallels between military action benefits and intelligence collection benefits, so we will use military actions as a substitute good when describing private benefits. Both military actions and intelligence gathering aim to preempt attacks that may put American citizens and interests at risks, and thus have an overlap in their positive outcome. Perhaps the most obvious private benefit to individuals is the

protection of the citizen's own life. Military action, such as basing troops overseas in high-risk areas, have been generally effective in deterring and preventing large scale attacks and promote regional stability (RAND, 2013). Overseas military intervention has the potential to deter and prevent terrorist cells from being able to plan attacks on American citizens. Likewise, intelligence gathering can supply information to defense leaders that can take action to prevent terrorist attacks. This prevention component of intelligence has a clear protection of life benefit to all those in the country that the intelligence collection affects.

Aside from the obvious protection of life benefit of intelligence gathering, we can associate intelligence gathering with the private benefit of the protection of individual quality of life. Again, we can draw this conclusion from the parallels between intelligence gathering and military intervention. If we make the assumption, that intelligence gathering in the post-9/11 era is intended to, and has been successful in, preventing terrorist attacks, then we can infer that intelligence gathering can help raise, or maintain the quality of life of an individual. For example, consider the case of the Boston Marathon Bombing on April 15, 2013. In a statement to the U.S. Congress a year after the event, the Boston police commissioner at the time helps frame the benefits of preventing terrorism by explaining the costs of the attack on an individual, citywide, and national scale. He describes the immediate costs of that day as including pain and injury to individuals in the blast radius of the pressure cooker bombs, as well as the negative impact the local area such as the extra stress on the local police force and hospitals (Boston Marathon Bombing, 2014). From that statement, we can infer that intelligence gathering and preventing terrorist attacks has the private benefit of taking stress off police work, and preventing more people from experiencing terror attack related injuries. Depending on the scale of the terrorist attack, this benefit has the potential to be quite large. In fact, after the 2001 terror

attacks, congress passed the Terrorism Risk Insurance Act which took some financial obligations from businesses affected, or completely compromised, by terror attacks. The bill states that the federal government will help pay for direct damages caused by terrorist attacks.

Positive Externalities and Social Benefits

As noted earlier, the likelihood of a consumer of intelligence being a victim of a terrorist attack is almost zero. Yet, the federal budget for intelligence agencies and intelligence activities is large. This is because the societal benefits of intelligence gathering are far more numerous than the private benefits to individual consumers. In fact, the theoretical social benefits of intelligence gathering have the potential to extend to everyone. This section will seek to explain how benefits and externalities that extends past the individual consumer's intelligence collection.

The CIA sates one of their primary purposes for collecting intelligence is not to combat terrorism with a military focus, but to inform politicians and provide necessary information to form policy (CIA, 2013). The CIA is in charge of preparing the President's daily brief and advising the NSC on matters dealing with foreign affairs and national security (Richelson, 2012 p22). Better informed policymakers are positive externalities through streamlined formation of law, and more efficient allocation of budget funds. Another positive externality associated with intelligence gathering is the improved foreign relations with our allies. After World War II, The United States entered into an agreement with New Zealand, Great Britain, Australia, and Canada to share sensitive information with one another and assist each other in intelligence activities in order to improve each individual country's national security. There is also a degree of information sharing involved with United Nations countries in cooperative struggles (Richelson,

2012 p22). Looking back at the statement made by the head of the NSA after the NSA leaks, we see that not all terrorist attacks prevented by that program would directly affect Americans. The majority of the 54 terror attacks that were cited in the congressional hearing were not going to involve Americans (Waterman, 2013). Thus, the attacks prevented by this program would have more international impact than on domestic soil, indicating a large prescience of an external benefit to intelligence gathering. Saving an ally from a terror attack shows strong external benefits of collecting intelligence by the U.S. government.

One last positive externality is the effect of terrorism on the financial sector and U.S. industry. The Organization for Economic Cooperation and Development estimates that the direct cost to the U.S. economy of the 9/11 terror attacks was about $27.2 billion. This figure includes physical damages, the cost of disruption where the attacks took place, and rebuilding expenses. The indirect costs, of the terror attacks were far greater and immeasurable. 9/11 showed us that s large-scale terror attack on the financial industry results in lower confidence for consumers and investors in private industry After 9/11 in the medium-term, the U.S. saw a reduction in spending and a higher propensity for consumer saving (Johnston, Nedelescu 2005).

In order to combat the economic recession after 9/11, the Federal government sent a great deal of money for aid and economic stimulus to New York and companies affected by the attack (Khasru, 2001). In addition, the nation saw a large increase in defense spending after the attacks in an attempt to prevent a terror attack from occurring again. In the five years following 9/11, U.S. defense spending rose from 3.5 percent of GDP to 4.6 percent by 2005 (World Bank). This increase can partially be attributed to the U.S. deployment of troops in Iraq in 2005, but the immediate rise in defense spending is largely attributed to 9/11 and the rise in defense spending to ramp up counterterrorism efforts. The increase homeland security spending in the decade after

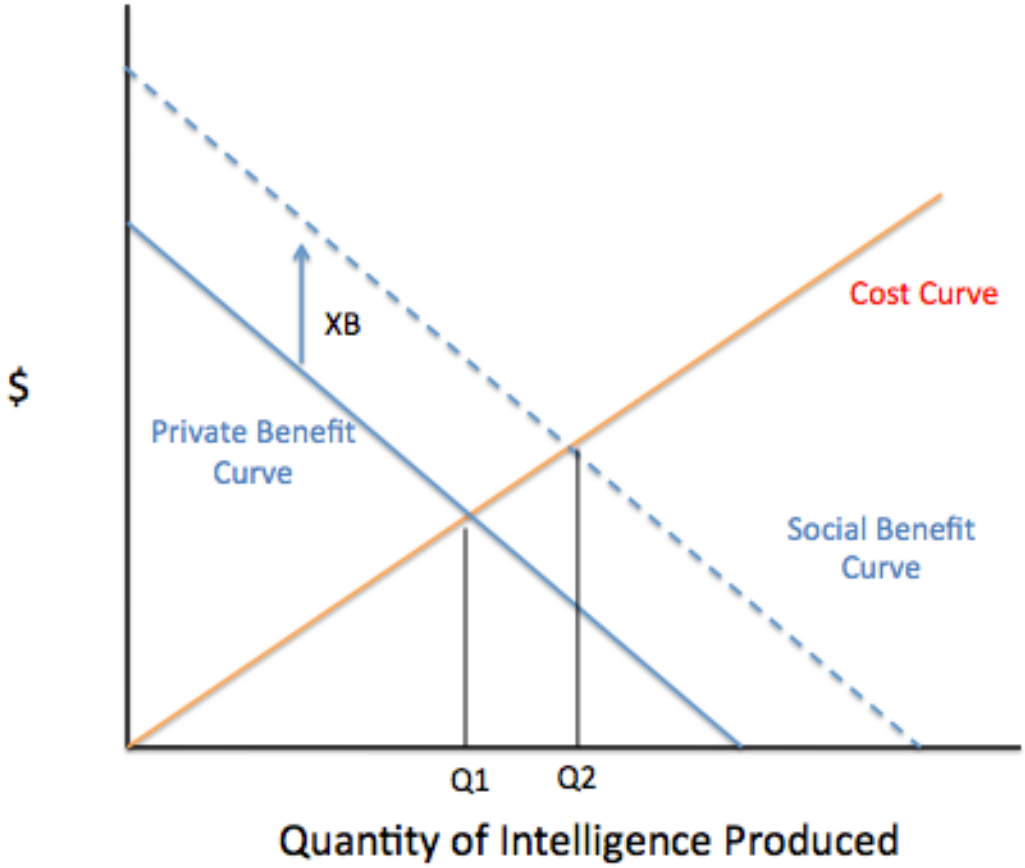
9/11 is estimated to be about $589 billion, not including any war costs associated with Iraq or Afghanistan. As another example of increased government spending the country saw a large-scale increase in terrorism prevention in airport security to prevent another airplane terror attack. The increased security and the increased travel restrictions after 9/11 cost the U.S. economy about $100 billion (Johnston, Nedelescu 2005). Avoided costs correlate with the external benefits of intelligence gathering. Because these discussed costs could have been avoided with intelligence gathering preventing 9/11, it can be inferred that the external benefits of producing intelligence are vast.

The cost of a terror attack has the potential to be very large. Including all of the war spending fallout after 9/11, the New York Times estimated that the 9/11 attacks cost this country $3.3 trillion(Carter, Cox, 2011). While this is one of the highest estimates and includes the government spending on the war in Iraq and Afghanistan, it shows that a terror attack has the potential to be a very high impact event. This amount of government spending, even spread over a decade, could've been used to improve critical infrastructure or help fund social programs at risk of being cut.

By our assumption, the avoided costs of a terror attack can be thought as the benefits of intelligence collection. The consumer of intelligence sees private benefits in the form of personal protection from attacks and their quality of life. However, society sees much greater, large-scale benefits such as more informed policy-makers, improved U.S. relations with other countries, and increased funds in the federal budget available for other federal programs (or perhaps lower taxes). All of these benefits have the potential to have far-reaching benefits in the end that positively affect American society has as whole.

With the introduction of positive externalities, associated with a good, it is likely that the market does not reflect the positive value of the good and thus the equilibrium in the market is not efficient. Figure 1 shows the market for intelligence and how the market may not internalize the positive externalities described associated with intelligence gathering and thus the market equilibrium under produces the quantity of intelligence. The private benefits are lower than the social benefits. More informed policymakers and avoided long run and institutional costs of terror attacks all contribute to the shift in the social benefit curve in Figure 1. In the figure, Q1 represents the private outcome of intelligence gathering in which no externality is realized. The positive externality, XB, shifts the benefits of intelligence gathering upward, and moves the equilibrium amount of intelligence gathering to Q2. The external benefit increases the amount of intelligence gathering that should take place.

Figure 1: Intelligence Market with Positive Externalities



Negative Externalities and Social Costs

Negative externalities lead to the overproduction of goods because the market cannot account for the extra costs associated with the externalities. In this economic model, the government agencies that collect intelligence are the producers, and the consumers of intelligence are the citizens of the U.S. protected by the intelligence activities. This cost is an individual cost to the taxpayers and is our most directly measurable. It was not until 2007 that the

IC started to declassify the amount of money it was appropriated by congress (Office of the Director of National Intelligence, 2016). In addition, it was not until 2011 that the IC had to disclose how much money they requested in each budget (MIP and NIP), so data on intelligence spending is very new with few data points (Office of the Director of National Intelligence, 2016).

Intelligence is not without external costs, especially in the wake of unauthorized disclosures. We have heard a great deal about intelligence oversight, and oversight reform. The intelligence community has a great deal of power, and thus requires a great deal of institutional support to ensure that all policies and laws are being followed. From an economic perspective, oversight and its potential intrusion on privacy and freedom is a large cost that the intelligence community imposes. It is important to note these oversight costs as these costs spillover to other government departments and agencies, and add additional costs to the production of intelligence products. While "oversight" can be a general term, we will use it to describe the costs that the intelligence community imposes on government institutions whose mission is outside of the intelligence community. Namely, the IC imposes costs on both the judiciary branch and the legislative branch of the U.S. Government.

The public disclosures of classified information to the media and public in the past few years have put into new light some of the costs that the country faces associated with intelligence collection. After the 2013 NSA leaks incident, there was a new wave of literature about the balance between civil liberties and security and where this line should be drawn for intelligence activities. The balance between privacy and security is not a new one; it is a debate that has been ongoing since the early attempts to ratify the U.S. Constitution with the Bill of Rights attached, putting more privacy in the hands of the people and less authority and power to the government

(Fidler, 2015, p21). Compromising on civil liberties is an external cost to intelligence gathering not internalized by the private intelligence market.

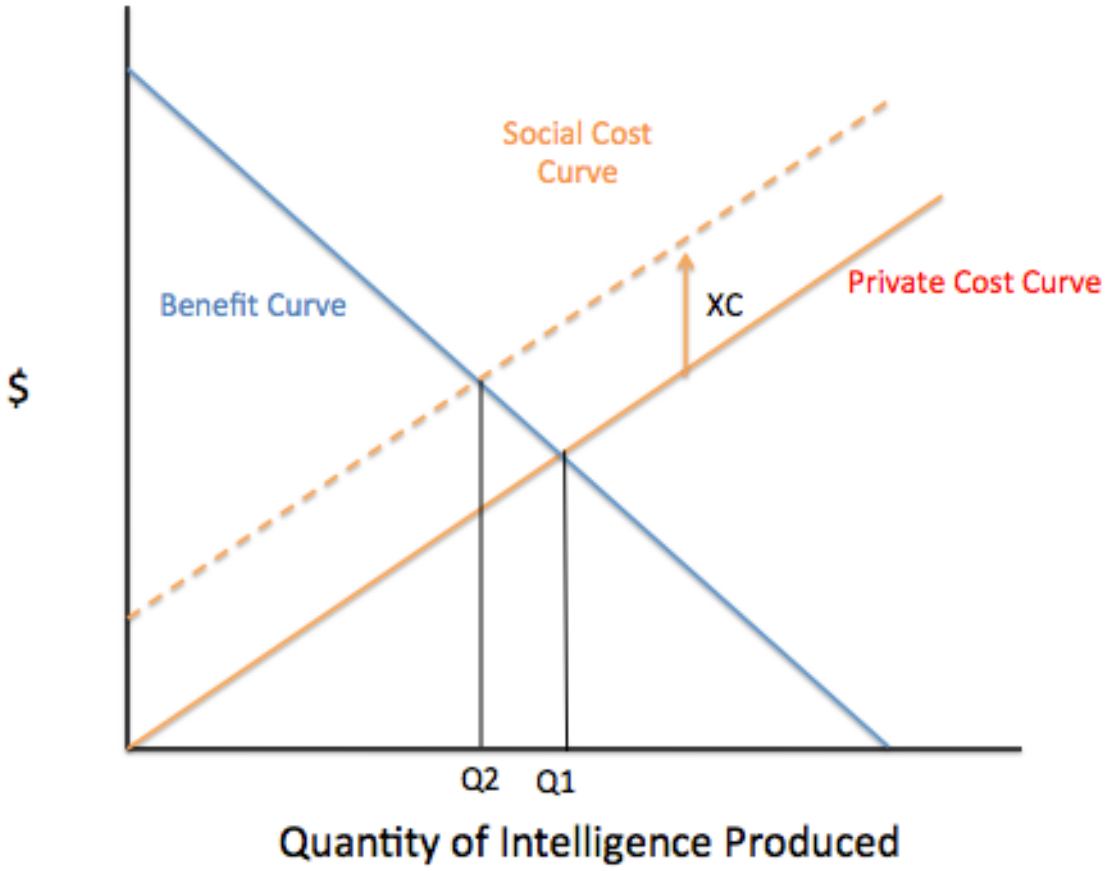
There are many cases in which security compromises liberties and freedoms, not necessarily related to intelligence. A simple, illustrative example of this is the rise in airport security after the 9/11 attacks (International Foundation for the Protection of Officer, 2003). In order to improve the safety of airline passengers, more security measures were put in place and item restrictions enacted in order for passengers to get on airplanes. The increased the security of passengers on planes left fewer options and added more time costs to flying by passengers. While airline rules don't constitute a violation of civil liberties, it does illustrate the tradeoff between security and privacy/freedoms.

After the 2013 NSA leaks incident, there was an effort from oversight bodies to ensure that intelligence processes did not violate the civil liberties. The cost of privacy is not necessarily quantifiable for an economic analysis of intelligence. However, it is simply important to note that privacy and civil liberties can be compromised with increased security and this could be categorized as a negative spillover/externality associated with increased intelligence production.

From a public economy perspective, it can be predicted that the U.S. government could collect too much intelligence than socially efficient because the civil liberties costs are positive. Perhaps this is exactly what the country saw when the FISC ruled that the actions of the NSA were "probably unconstitutional" prompting a review of intelligence collection practices with the lens of protecting civil liberties and privacy (Fidler, 2015, 20). A common proposed solution to decrease the magnitude of this negative externality is to increase the effectiveness of oversight bodies (Fidler, 2015, 50-51).

In the case of intelligence, the public goods market may lead to an overproduction of intelligence because the negative externalities described would not be internalized. The free market would lead to the government producing an amount of intelligence that is privately efficient, but not socially efficient. With the addition of the negative externalities such as oversight costs and privacy costs the social costs higher. Figure 2 shows the market for intelligence with a negative externality, where the market production of intelligence is at Q1. The external costs of intelligence gathering are represented by XC, which shifts the cost curve up. After the costs are internalized, the socially efficient quantity is at Q2.

Figure 2: Intelligence Market with Negative Externalities



Externalities Analysis

The argument could be made that there are both positive and negative externalities associated with intelligence gathering. For a public goods model, it is important to discover if the overall externality effect is negative or positive. Figures 3 and 4 show the market for intelligence in which there is both a positive and negative externality present, and there are social shifts in the costs and benefits curves. In Figure 3, the overall externality effect is negative, and we see that the private market overproduces intelligence. In this case, the social equilibrium, Q2, is lower than the private equilibrium, Q1. If this figure accurately reflects reality, the government should produce less intelligence. In Figure 4, we see the overall externality effect is positive. Here, the social optimum, Q2 is higher than the private outcome, Q1. The private market under produces intelligence. If this figure accurately reflects reality, the government should produce more intelligence. Without concrete data available or more insight on the overall externality associated with intelligence gathering, it is impossible to state the overall externality effect on intelligence. More information is needed to determine the equilibrium and the factors that shift the social costs and benefits curves, in order for the government to effectively control the market for intelligence and ensure efficiency.

Figure 3: Overall Negative Externality Effect

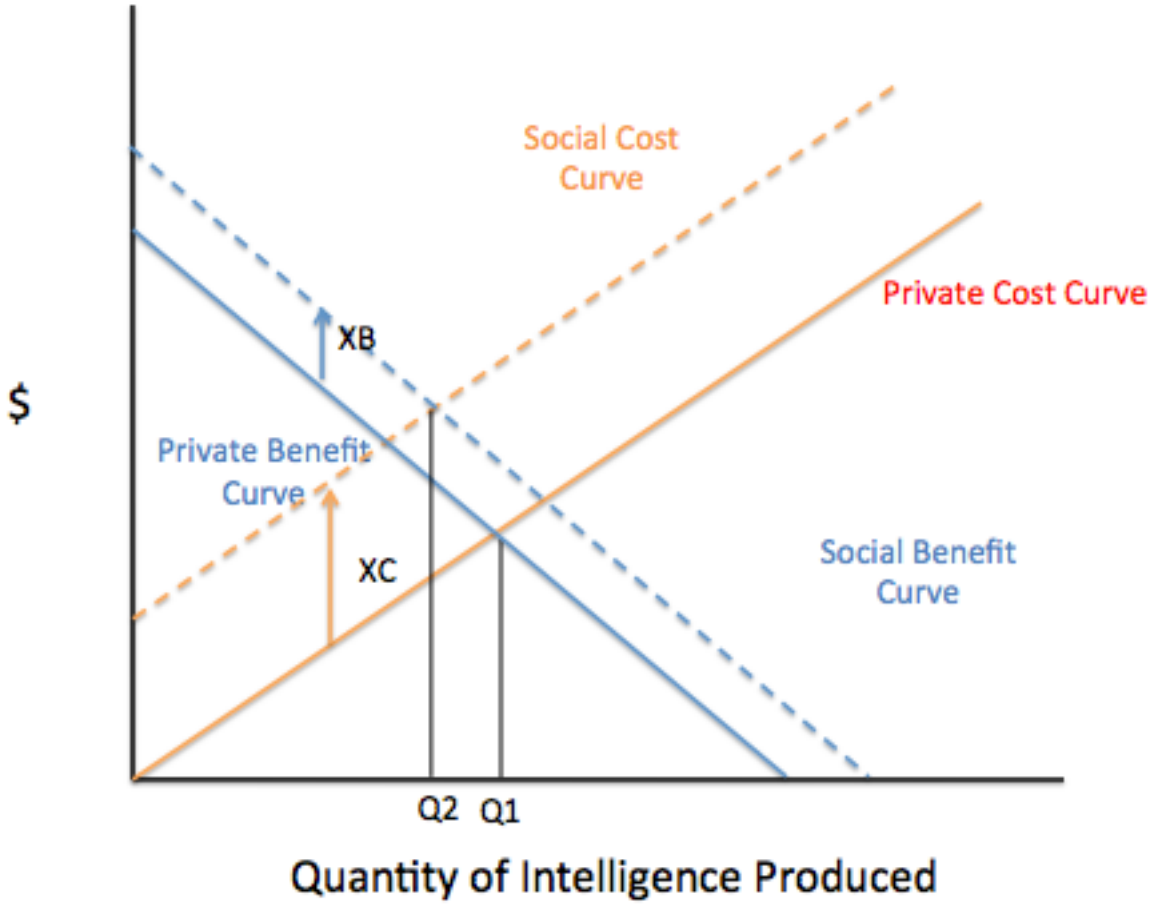
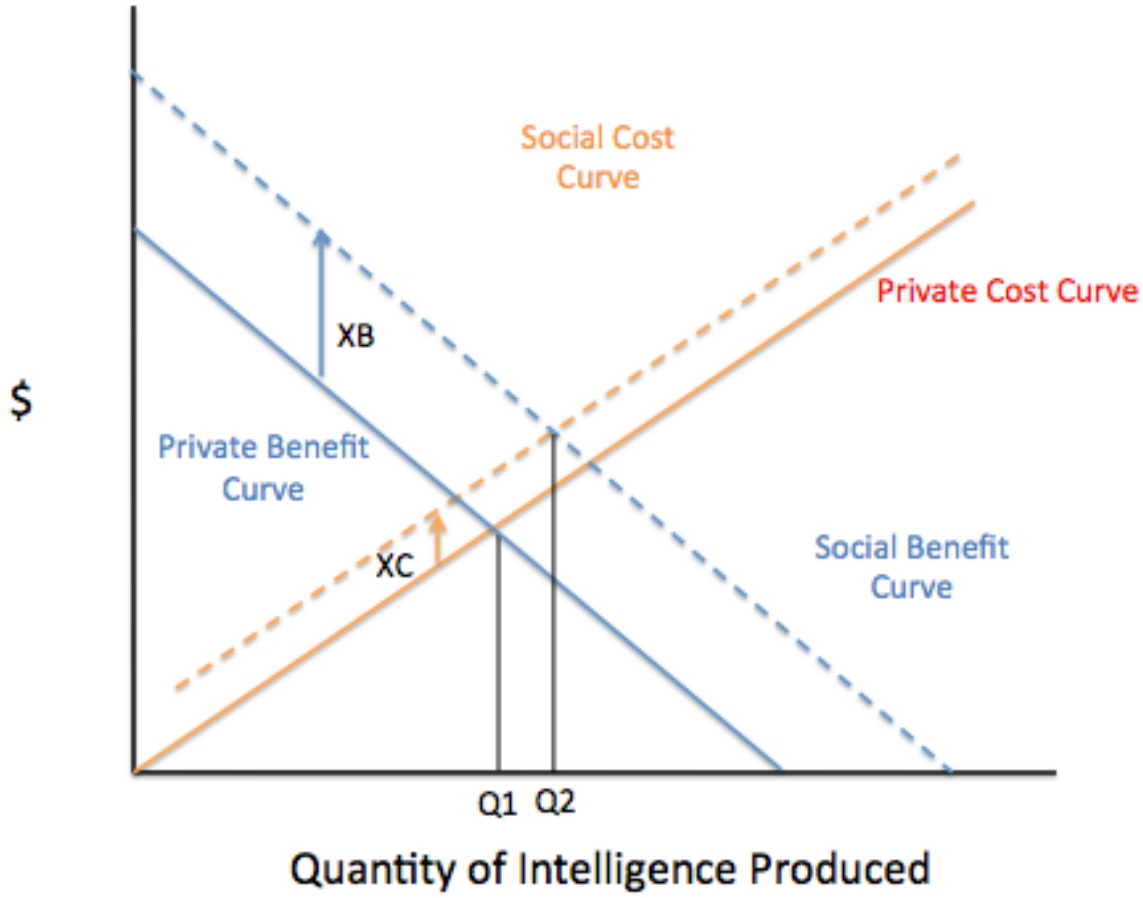


Figure 4: Overall Positive Externality Effect



Chapter 4: Risk Analysis of Intelligence

Economic theory has been useful in helping understand intelligence production from the point of view of society. A risk analysis perspective adds to our economic analysis of intelligence as an economic good. Risk analysis can look at the costs and benefits of intelligence from an event perspective. The model so far looks at the benefits and costs of intelligence gathering in the aggregate. An event theory helps provide perspective on the specific scenarios that lead to costs and benefits associated with intelligence gathering. This section describes the practice of risk analysis and risk management as an alternative view. Risk analysis will help describe the potential value of a single piece of intelligence. Traditional risk can be defined as a function of the likelihood of an undesired event occurring and the impact of the event if it did occur (NIST, 2003). Thus, a potential attack that has a high likelihood assessment, and a high impact, would have a very high risk value. A potential attack that would cause large damages but is very unlikely to ever happen would have a much lower risk value. Many risk analysis frameworks will multiply the likelihood of an event by the dollar impact the event would have in order to compute a quantitative risk. For example, a terror attack with a .1 percent chance of happening that would cost $3 billion dollars in damages would compute to an expected risk value of $3 million. Appendix C shows a matrix that illustrates the probability and impact components of risk.

Risk analysis is useful in developing relative risk scores/values of similar events. Traditionally, a wide range of scenarios will be considered in a comprehensive risk analysis. They will be ranked and prioritized, and controls will be put in place to reduce the risks (NIST, 2003). Leading risk analysis expert, Yacov Haimes uses a risk analysis framework that seeks to answer three key questions: “What can go wrong? What is the likelihood of this happening? And

what are the consequences?" (Haimes et al. 2002). The goal of risk analysis is to help inform decision-making. For our intelligence perspective, risk analysis can be applied in several ways. The following sections will discuss intelligence and risk from two perspectives: The value of intelligence in assessing terrorism risk and the risk of gathering intelligence itself

Intelligence Value in Terrorism Risk

Measuring the risk of terrorism is a growing science that can have many policy implications. After the passage of the National Security Act of 1947, senior government officials can request national intelligence estimates (NIEs), which are documents that give background on a key intelligence priority or issue (Council on Foreign Relations, 2008). Presidential cabinet members can request an NIE on the threat of the Islamic State of Iraq and the Levant (ISIS) on the homeland, the terror climate in Iraq, or the prospects of Chinese power in the next decade. These reports would combine intelligence from all agencies and departments that have any input on the issue requested. These estimates are risk analysis documents that assess the current state of a region, event, or organization, and then project the future state of the topic, with potentially outcomes and scenarios based on the intelligence available at the time. Hundreds of NIEs have been written in the past few decades (Council on Foreign Relations, 2008). More recently these reports have dealt with terror groups. These documents are used in making key policy decisions. Intelligence products are the most important inputs into the NIE production process, thus the role of intelligence is critical in the risk assessment and policy making process on foreign relations issues.

From an economic perspective, we are interested in the benefits that intelligence gathering provides in the risk assessment process as to fully understand the expected value that intelligence products provide. As stated earlier, risk analysis processes break down risk into the likelihood and impact of an event. While the specifics of terror risk methodologies differ, they generally seek to assess whether a threat exists to an area (likelihood), whether a target is vulnerable (likelihood) and what damage would result if the attack were carried out (impact) (RAND, 2013).

Intelligence can be used to assess the likelihood of a location becoming a target for a terror attack, and the likelihood that a terror group will carry out an attack on a target. For example, SIGINT can be used to collect communications of many different terror groups to determine which areas are more likely to be targeted by terror groups. The RAND corporation assesses that New York City has the highest relative likelihood of encountering a terror attack, followed by Chicago, Los Angeles, and San Francisco (RAND, 2013). This likelihood can also be calculated using historical analysis, inferences based on population area, and how easy it would be for terrorists to attack the target.

The Cuban Missile Crisis can help explain the value of intelligence in determining the likelihood of an attack happening on U.S. soil. In 1962, the U.S. government had unconfirmed intelligence that suggested the Soviet Union was using Cuba to stage an attack on the U.S., breaking the Cold War stalemate. Officials required more intelligence before acting, so imagery intelligence was collected from Cuba. High altitude U-2 airplanes flew over Cuba and showed that the intelligence was indeed true. The Soviet Union was building missile silos in Cuba (Federation of American Scientists, 1997). This single piece of intelligence was informative in calculating the likelihood of an attack occurring in two ways. First, this intelligence helped

determine the location of the attack. The images showed the missiles that would be fired were intermediate range missiles (unlikely to reach the northwest portions of the U.S.). This made the southeastern portion of the U.S. the most likely location of an attack. This intelligence was crucial in assessing the probability component risk of an attack based on locations in the U.S. In addition, the intelligence informed policymakers that the likelihood of the Soviet Union shooting missiles at the U.S. had increased. Ultimately it is unknown whether the Soviet Union was actually going to fire these missiles, but the U.S. used this intelligence, assessed the risk of an attack as high probability, and acted to preempt and avoid the attack. Without this intelligence, the outcome could have been much worse and may have resulted in a very costly war.

In addition to contributing to analyzing the likelihood of a terror attack, intelligence can also contribute to assessing the impact of an event. This is true in the Cuban missile crisis example. The images gathered from intelligence collection showed information about the types and quantities of missiles pointed toward the U.S. This helped determine the impact of any potential attack. If there was just one missile moved to Cuba, the impact would have been relatively low. However, the intelligence produced images of many missiles (Federation of American Scientists, 1997) which greatly increased the potential impact of the event.

Risk Analysis of Intelligence Gathering

Risk analysis principles provide a method to gain a more complete picture of the costs associated with intelligence gathering. Risk analysis frameworks first seek to determine the list of possible failures within a specific context (Horowitz, Haimes, 2003). So we begin our risk

analysis by asking, “what can go wrong when we gather intelligence?” We can investigate this by looking at the past and analyzing what has already gone wrong. The 2002 weapons of mass destruction report about Iraq is a good case.

In September 2002, President Bush asked Congress for the authority to use military action against Iraq. This action was taken because the U.S. IC concluded that Iraq was building its WMD program (Council on Foreign Relations, 2008). Military action was intended to preempt the use of these weapons and had public support. After using military action, it was determined that the reports were based on poor intelligence. In an oversight investigation report, the Senate determined that intelligence officers suffered from bias, groupthink, and poor analytic techniques that turned an assumption of Iraq WMDs into a conclusion. The IC misinterpreted ambiguous evidence and made conclusions from poor judgments (Council on Foreign Relations, 2008).

Incorrect conclusions from intelligence can cause large costs. Upon initial military action, the Bush administration projected the cost of the Iraq War to be $50-60 billion. Conservative estimates after the war ended put the total cost at over $800 billion (Childress, 2013). This figure shows that poor analysis practices pose huge risks for taxpayers. While the probability of a misstep on this scale is assumed small based on the infrequency of published intelligence errors, the impact is very large and thus is an important risk to note. Steps were taken after the Senate report to reduce this likelihood. For example, the NIE process was improved to increase the probability of correct conclusions. In addition, the Bush administration promoted information sharing among components of the IC as part of its agenda, attempting to increase the likelihood that conclusions from intelligence would be accurate and consistent.

Furthering our analysis, let us make the assumption that the risk of incorrect conclusions is more likely to occur when too little or too much intelligence is collected in the IC. If too little intelligence is collected, there are not enough pieces of information for analysts to draw the correct conclusion for policymakers to act upon. If too much intelligence is collected, the IC structure is stressed, information sharing and cooperation is reduced, and the likelihood of a misconclusion. Thus our risk analysis framework not only gives us more clues as to the costs of intelligence gathering (incorrect conclusions) but also indicates that an equilibrium exists for an optimal quantity of intelligence gathered, consistent with traditional optimization theory. Figure 5 shows the theorized relationship between intelligence collection quantities and the probability of an intelligence failure. There exists an optimal quantity of intelligence gathering that minimizes the probability of a poor intelligence conclusion (Q*). QA represents a case in which the probability of an intelligence failure is higher than optimal because the IC is collecting too little intelligence. This can be related to a pre-9/11 era where not enough intelligence was collected, leading to incomplete information and a terror attack. QB represents an overproduction of intelligence resulting in a higher than optimal probability of an intelligence failure. This point could be used to describe the post-9/11 era with the expansion of the IC and increase in intelligence production. Too much production led to incomplete and inaccurate analysis, ultimately resulting in an intelligence failure of the 2003 WMD report.

Figure 5: Probability of Poor Intelligence Conclusions

From the sheer increase in size of the IC after 9/11, it will be assumed that it is unlikely that too little intelligence was collected. It is also possible that the risk of incorrect intelligence collection provides a negative externality when too much intelligence is produced. Our risk analysis perspective shows that the risk of this type of intelligence failure increases when intelligence is overproduced. Using this logic with the fact that 9/11 caused a large increase in intelligence production, our analysis explains the factors that led to the incorrect 2002 report.

Chapter 5: Blind Consumption and Principal-Agent Theory

Principal-Agent theory has its own application in our intelligence as an economic good concept. This theory started from contract theory as a way to theorize information asymmetries and imbalances between two parties in a contract (Andersen et al. 2008). Logically, this theory is certainly useful, as our market for intelligence contains a great deal of information asymmetries. We have already looked at the relationship between taxpayers (principal) and the government institutions that collect intelligence on behalf of the taxpayer's wellbeing. These include the lack of taxpayer knowledge about the intelligence market and their inability to provide input on their own behalf to influence the intelligence process. There could also be asymmetries between the president and the IC. In this case, the policy setters are the principals and the Intelligence Community are agents that act on behalf of the policy setters. Information issues affect this relationship and can lead to economic inefficiencies. This section will use a principal-agent framework to identify and remedy these issues.

Taxpayer-Intelligence Community Relationship

To better understand the principal-agent relationship that exists between the consumer of intelligence, the taxpayers, and the producers of intelligence, the IC, we can draw from parallels from the healthcare field. This relationship is very similar to that between a patient with a health issue, and a medical professional tasked to resolve the medical issue. The parallels between these two relationships are as follows:

(1) Both the taxpayer and the patient face a potentially low-probability, high-impact event (potentially fatal illness or terror attack).

(2) Neither the taxpayer nor the patient has the skill to eliminate the threat each face.

(3) Both the medical professional and the IC are delegated to eliminate threats on behalf of their respective principals.

(4) Both the medical professional and the IC have special expertise and hidden information that their principal's are not able to acquire.

(5) Intelligence gathering and medical diagnoses require analysis and can result in a less than 100 percent success rate, thus they may not optimize the utility of the principal.

(6) Neither the patient or the taxpayer can be certain that their agents have resolved the threat(s) they face.

Comparing the taxpayer-IC relationship to the doctor-patient relationship assists in providing a thorough analysis of the information issues that may arise in this type of relationship. In the doctor-patient relationship, we see many information issues and inefficiencies. The patient must rely on the doctor and his/her high medical skill in order to resolve the threat the patient faces. If the patient no longer faces sickness, he/she does not know if it is the result of doctor intervention, or their own immune system/other environmental factors (Ludwig, 2009). In addition, it is unknown to the patients whether or not the doctors are acting on the patient's best interest, or the doctors'. In the relationship between a doctor and a patient, it may be the case that the doctor sacrifices quality of healthcare for their own interest and to improve their own utility (Ludwig, 2009).

The issues identified in this relationship can be paralleled in the relationship between the taxpayer and the IC. For example, the taxpayers must rely on the IC in order to protect their lives from terror and other threats. When a taxpayer lives a day without being harmed in any way from terrorism, they are not sure if their safety can be attributed to the success of the IC, or other factors such as the environment or even chance. Finally, it is unknown to the taxpayer if the IC is acting in the taxpayer's best interest, or the IC's best interest. If there exists the potential for a scenario where it would be too costly for the IC to act on behalf of a taxpayer, and that the utility of the IC would be decreased, then there exists the possibility that the IC does not act in the taxpayer best interests.

One solution to the information issues that exist in the doctor-patient relationship is the publishing of the overall quality of the care given by the doctor to the patient (Ludwig, 2009). While patients have the opportunity to choose their medical care professional based on their quality, the taxpayers do not have the option to choose their IC provider directly. However, taxpayers can vote in a President and policymakers that will nominate and approve higher quality intelligence officials. Taxpayers are able to indirectly affect the employment of intelligence officials and can remove an ineffective intelligence official from office. Reports that would indicate the success rate of the IC and reflect the quality of product they give their consumers would help improve this relationship and lead to more efficiencies in the market, not completely producer dominated. However, this brings about the paradox of the nature of classified information in intelligence. This paradox makes it difficult to produce quality reports for the IC.

Internal Intelligence Community Relationship

In this relationship, the principal role is held by as the leaders/agenda setters of the Intelligence Community, and the agents are the different components of the IC. This relationship can also be compared to the healthcare field when we look at the internal relationships of a hospital. Within a hospital, a hospital board and the departments within the hospital have a principal-agent relationship. The hospital board plays the role of the principal, and the departments within the hospital are the agents acting to produce the outcomes associated with the hospital (Ludwig, 2009). In this relationship, the board is attempting to maximize their own objective function by delegating responsibility to the departments within the hospital. Each department has its own, potentially different function. They also have more specialized knowledge of their own abilities. Depending on incentives and the workings of the hospital, it is possible for the departments to act in their own best interest, maximize their own well-being, which can harm the well-being the board (Ludwig, 2009).

Likewise, the President (and Director of National Intelligence) set intelligence priorities, but delegate the work to the different agencies within the IC in order to maximize the President's utility, conceivably measured in public approval and voting support. However, if there exists a possibility that the utility of each agency is not aligned with the utility function of the President, then the agencies could act in their own best interests and a less than optimal outcome would be realized. A common criticism of the Intelligence Community after the 2013 NSA leaks was that the IC was not acting in the best interests of the public by violating privacy rights and that the increased intelligence value from programs leaked was not worth the violation of these rights. Assuming the President represents the will of the Public, we can see the possibility that the

components of the IC were acting in their own best interests to maximize their utility and efficiency, without complete regard of the utility of the President (and in turn, the public will).

Policy Solutions

With a principal-agent framework, we are able to highlight some of the information issues in the market for intelligence. From a policy perspective, there are ways in which it is possible to fix some of these information asymmetries in order to increase the likelihood of an efficient outcome.

In general, more transparency would help fix many of the issues. As stated earlier, if the IC was rated on quality of their product a more efficient outcome would be realized. A practical way to implement quality ratings would be through congressional oversight. While the common taxpayer is unable to rate the quality of the IC on their own (due to the classified nature of intelligence), policymakers who are voted in by taxpayers are able to do just that. The House and Senate both have oversight committees, but neither publishes regular quality ratings for the effectiveness of the IC. These ratings would put pressure on the IC to ensure their actions are aligned with the best interests of the public.

Another possible policy solution to help both of the relationships listed above would be benchmarking. Benchmarking would consist of setting goals for the IC, most likely coming from Congress, that they must meet in order to avoid repercussions. This is a common technique imposed throughout the public sector (Andersen et al., 2008) and can have its use for the Intelligence Community. Imposing benchmarks that represent the will of the President and the general public will help ensure the IC acts to maximize the utility of the public. If a benchmark

isn’t met, components of the IC can lose funding, which would significantly harm the efficiency of the IC. Imposing benchmarks would add a large cost to not maximizing the public’s utility and would reduce the incentive for the IC to prioritize their own efficiency over the welfare of the public.

Policy solutions that would increase the transparency between the Intelligence Community, the President and the public would help remove the inefficiencies that result from the inherent information asymmetries in the relationships between these parties. Quality checks and benchmarks would help achieve this goal and would bring the market for intelligence closer to its equilibrium.

Conclusion

Studying national intelligence collection from an economic perspective might be the key to determining the fix to the intelligence issues the U.S. has seen in the past two decades. The current structure of the IC, and the hidden nature of the outcomes of intelligence leads to information asymmetries between the taxpayer consumer and the government producers of intelligence. In addition, the nature of the public good aspect of intelligence, namely the externalities associated with intelligence collection and processing is unknown to the consumers of intelligence. In order for the market for intelligence to reach equilibrium, the producers and consumers of intelligence must understand the overall externality effect of intelligence gathering.

Overall, the information asymmetries in the market for intelligence must be reduced in order for the market to reach equilibrium. Today, the majority of consumers do not know exactly what product their taxpayer dollars are paying for, and have little understanding of the intelligence landscape in the U.S. Because of this, the government producers of intelligence have had complete control of the market for intelligence, and we have seen several intelligence failures since the turn of the century. It is of upmost importance for policymakers to find a solution that increases consumer awareness of the intelligence process, as well as increasing the ability of consumers to provide input in the aggregate intelligence collection in the U.S. Consumer understanding of intelligence, and the outputs of their investments in the intelligence community is the first step in allowing this market to reach equilibrium.

BIBLIOGRAPHY

Andersen, B., Henriksen, B., & Spjelkavik, I. (2008). Benchmarking applications in public sector principal-agent relationships. *Benchmarking, an International Journal 15*(6), 723-741., from doi:http://dx.doi.org/10.1108/14635770810915913

Belfer Center for Science and International Affairs. (2009, July). "Congressional Oversight of the Intelligence Community" Retrieved February 29, 2016, from http://belfercenter.ksg.harvard.edu/publication/19146/congressional_oversight_of_the_intelligence_community.html

Boston Marathon Bombings, One Year On: Look Back to Look Forward: Hearing before the Committee on Homeland Security, House of Representatives, One Hundred Thirteenth Congress, Second Session (2014, April 9). Retrieved from http://www.heinonline.org/HOL/Page?handle=hein.cbhear/fdsysaaym0001&id=1&size=2&collection=congrec&index=cbhear

Carter, S., & Cox, A. (2011, September 07). One 9/11 Tally: $3.3 Trillion. Retrieved from http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=1

Childress, S., & PBS. (2013, March 18). The Iraq War: How We Spent $800 Billion and Counting. Retrieved March 03, 2016, from http://www.pbs.org/wgbh/pages/frontline/iraq-war-on-terror/the-iraq-war-how-we-spent-800-billion-and-counting/

Cole, J. (2014). Reform Of The Foreign Intelligence Surveillance Courts: Brief Overview, from http://www.heinonline.org/HOL/Page?handle=hein.crs/crsmthaaalv0001&id=1&size=2&collection=congrec&index=alpha/R_crs#

Council on Foreign Relations. (2008). National Intelligence Estimates., from http://www.cfr.org/iraq/national-intelligence-estimates/p7758#p5

Federation of American Scientists. (1997, March 23). Cuban Missile Crisis., from http://fas.org/irp/imint/cuba.htm

Federation of American Scientists. U.S. Intelligence Budget Data. (2016) from https://fas.org/irp/budget/

Fidler, D. P. (2015). The Snowden reader. from http://site.ebrary.com/lib/pennstate/reader.action?docID=11040206

Foreign Intelligence Surveillance Court. (2016)., from http://www.fisc.uscourts.gov/

Haimes, Y. Y., Kaplan, S., & Lambert, J. H. (2002 April). Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling., from http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.00020/full

Horowitz, B. M., & Haimes, Y. Y. (2003, March 8). Risk-Based Methodologies for Scenario Tracking, Intelligence Gathering, and Analysis for Countering Terrorism. Retrieved March 03, 2016, from http://onlinelibrary.wiley.com/doi/10.1002/sys.10043/epdf

International Foundation for Protection Officers. (2003, December). The Evolution of Airline Security Since 9/11 - International Foundation for Protection Officers. Retrieved April 02, 2016, from http://www.ifpo.org/resource-links/articles-and-reports/protection-of-specific-environments/the-evolution-of-airline-security-since-911/

Johnston, R. B., & Nedelescu, O. M. (2005, March). The Impact of Terrorism on Financial Markets (International Monetary Fund). Retrieved from http://www.imf.org/external/pubs/ft/wp/2005/wp0560.pdf

Khasru, B. Z. (2001, September 17). Questions of investor confidence as business copes with terrorism. Fairfield County Business Journal, 40.38. Retrieved from http://search.proquest.com/docview/216402347?pq-origsite=summon&accountid=13158

Lowenthal, M. (2015). Intelligence: From secrets to policy 6th edition. Washington, D.C.: CQ.

Ludwig, M., Van Merode, F., & Groot, W.. (2010). Principal agent relationships and the efficiency of hospitals. *The European Journal of Health Economics, 11*(3), 291–304., from http://www.jstor.org/stable/40730763

National Institute of Standards and Technology. (2002, July). Risk Management Guide for Information Technology Systems., from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Morton I. Kamien, Nancy L. Schwartz, Donald John Roberts, Exclusion, externalities, and public goods, Journal of Public Economics, Volume 2, Issue 3, 1973, Pages 217-230

Oakland, W. (1987) Chapter 9 Theory of public goods, *Handbook of Public Economics, Elsevier, Volume 2*, from http://www.sciencedirect.com/science/article/pii/S1573442087800046?np=y

Office of Management and Budget. (2016). Meeting our Greatest Challenges: National Security and Leadership. from https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/security_and_leadership.pdf

Office of Management and Budget. (2016) The President's 2015 Budget. Retrieved February 20, 2016, from https://budget2017.whitehouse.gov/#!/year/2015/revenue/0/function_title

Office of the Director of National Intelligence. (2016, February 6). Intelligence Community Budget. Retrieved February 29, 2016, from http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/ic-policies-2?highlight=WyJidWRnZXQiXQ

Office of the Under Secretary of Defense. (2014, April) “National Defense Budget Estimates for FY 2015”., from http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/FY15_Green_Book.pdf

The Permanent Select Committee on Intelligence | The Permanent Select Committee on Intelligence. (2016). Retrieved February 29, 2016, from http://intelligence.house.gov/

Pigou, A. C. (1920). The Economics of Welfare

RAND Corporation. (2007). Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection. Retrieved March 03, 2016, from http://www.rand.org/pubs/technical_reports/TR386.html

RAND Corporation (2013). Summary - Overseas Basing of U.S. Military Forces. Retrieved from http://www.rand.org/pubs/research_reports/RR201.html

Richelson, J. (1995). The U.S. intelligence community. Retrieved from https://libraries-psu-edu.ezaccess.libraries.psu.edu

Samuelson, Paul A.. “The Pure Theory of Public Expenditure”. The Review of Economics and Statistics 36.4 (1954) from http://www.jstor.org/stable/1925895?pq-origsite=summon&seq=1#page_scan_tab_contents

U.S. Department of State. (2012, July 31). “Terrorism Deaths, Injuries, Kidnappings of Private U.S. Citizens 2011” from http://www.state.gov/j/ct/rls/crt/2011/195556.htm

The White House. (2016). National Security Council. Retrieved March 04, 2016, from https://www.whitehouse.gov/administration/eop/nsc/

University of Maryland (2015). Global Terrorism Database. from: http://www.start.umd.edu/gtd/

Waterman, S. (2013, October 2). NSA chief’s admission of misleading numbers adds to Obama administration blunders. Retrieved from http://www.washingtontimes.com/news/2013/oct/2/nsa-chief-figures-foiled-terror-plots-misleading/

The Washington Times

What We Do. (2013, April 23). Central Intelligence Agency, from https://www.cia.gov/about-cia/todays-cia/what-we-do

World Bank. Military Expenditure (% of GDP) Data Set. from data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS

Appendix A: Glossary of Acronyms

CIA: Central Intelligence Agency

DEA: Drug Enforcement Agency

DHS: Department of Homeland Security

DIA: Defense Intelligence Agency

DNI: Director of National Intelligence

DoD: Department of Defense

FBI: Federal Bureau of Investigation

FISC: Foreign Intelligence Surveillance Court

GEOINT: Geospatial Intelligence

HIPSCI: House of Representatives Permanent Select Committee on Intelligence

HUMINT: Human Intelligence

IC: Intelligence Community

IMINT: Imagery Intelligence

IRTPA: Intelligence Reform and Terrorism Prevention Act

MASINT: Measures and Signatures Intelligence

MIP: Military Intelligence Program

NGA: National Geospatial Agency

NIE: National Intelligence Estimate

NIP: National Intelligence Program

NRO: National Reconnaissance Office

NSA: National Security Agency

NSC: National Security Council

ODNI: Office of the Director of National Intelligence

SIGINT: Signals Intelligence

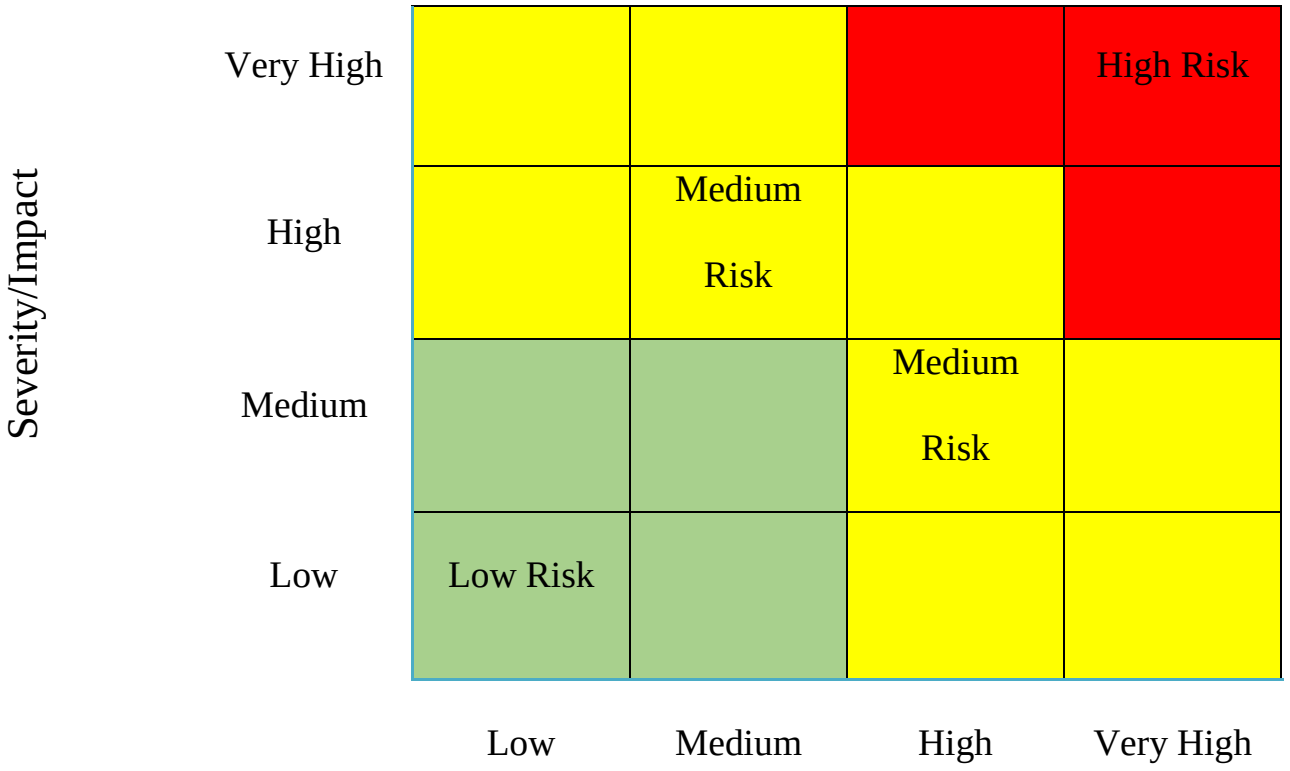
SSCI: Senate Select Committee on Intelligence

Appendix B: NIP and MIP Spending by Year

Fiscal Year	NIP Budget Requested	NIP Budget Appropriated	MIP Budget Requested	NIP Budget Appropriated	Total Appropriation
2017	$53.5 Billion		$16.8 Billion		
2016	$53.9 Billion		$17.9 Billion		
2015	$50.4 Billion	$50.3 Billion	16.6 Billion	$16.5 Billion	$66.8 Billion
2014	$52.2 Billion	$50.5 Billion	$14.6 Billion	$17.4 Billion	$67.9Billion
2013	$52.6 Billion	$49.0 Billion	$19.2 Billion	$18.6 Billion	$67.6 Billion
2012	$55.0 Billion	$53.9 Billion		$21.5 Billion	$75.4 Billion
2011		$54.6 Billion		$24.0 Billion	$78.6 Billion
2010		$53.1 Billion		$27.0 Billion	$80.1 Billion
2009		$49.8 Billion		$26.4 Billion	$76.2 Billion
2008		$47.5 Billion		$22.9 Billion	$70.4 Billion
2007		$43.5 Billion		$20.0 Billion	$63.5 Billion

Data from: The Office of the Director of National Intelligence

Appendix C: Risk Matrix



ACADEMIC VITA

Academic Vita of Mark Ryan
Markry5258@gmail.com

Education
Majors and Minor: Economics (B.S) and Security Risk Analysis (B.S) with a minor in Political Science
Honors: Economics
Thesis Title: National Intelligence: An Economic Perspective
Thesis Supervisor: Colin Knapp

Work Experience:

Date: 2014-2016
Title: Penn State Resident Assistant
Description: Promote a safe and welcoming community for first-year Penn State students
Institution/Company: Pennsylvania State University

Awards:

Dr. Raymond E. Lombra Scholarship in Economics

PNC Technologies Scholarship Award

Schreyer Academic Excellence Award

Penn State University Deans List

Community Service Involvement:

Penn State Resident Assistant 2014-2016

Penn State THON Merchandise Captain 2015-2016

Language Proficiency: English