THE IMPACT OF CYBER ESPIONAGE: CHANGING PERCEPTIONS WITH THE US VIS-A-VIS THE TRANSATLANTIC

by

Cliffard A. Patton

A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Master of Science
Conflict Analysis and Resolution
Master of Arts
Conflict Resolution and Mediterranean Security

Committee:

_____ Chair of Committee

_____

_____

_____ Graduate Program Director

_____ Dean, School for Conflict Analysis and Resolution

Date: _____ Spring Semester 2015
George Mason University
Fairfax, VA
University of Malta
Valletta, Malta

The Impact of Cyber Espionage: Changing Perceptions with the US vis-a-vis the Transatlantic

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at George Mason University, and the degree of Master of Arts at the University of Malta

by

Cliffard A. Patton
Bachelor of Arts and Bachelor of Science
Florida State University 2012

Director: Calleya, Stephen, Professor
Mediterranean Academy of Diplomatic Studies

Spring Semester 2015
George Mason University
Fairfax, Virginia
University of Malta
Msida, Malta

DEDICATION

This is dedicated to my Mother who I love dearly. She has always supported me in all my endeavors and more importantly she has always been there for me through the easy times and the hard times. To my brother Richard and Grandpa Baker have also been beacons of light in my journey of life. I cannot leave them out of my dedication. Finally, to my loving bloodhound Zahara who has spent many nights by my desk and who successfully got me out of my chair often to go play with her.

ACKNOWLEDGEMENTS

I would like to think Professor Calleya at the MEDAC Institution at the University of Malta and Michael English, our program supervisor from the S-CAR Institution at George Mason University. Both gentlemen were instrumental throughout my masters degree program and key to my success. I would also like to thank all of the friends, professors and supporters throughout my educational path from my humble beginnings at Brevard Community College to Florida State University and within the George Mason University dual degree program with the University of Malta. There are too many names of great friends and profound supporters for me to add here. But I must mention the BCC Student Government Association, the Pi Gamma Mu Zeta Chapter at FSU and the CRAMS group at the GMU/UM dual degree program. Finally, thanks to Kurt Lorenzini and Regal Custom Painting Inc. who supported my drive in continuing my education.

TABLE OF CONTENTS

ABSTRACT

THE IMPACT OF CYBER ESPIONAGE: CHANGING PERCEPTIONS WITH THE US VIS-A-VIS THE TRANSATLANTIC

Cliffard A. Patton, MA/MS

George Mason University, 2015 and The University of Malta 2014

Dissertation Director: Dr. Stephen Calleya

This thesis describes an international impact of cyber espionage with an emphasis on the United States of America and its National Security Agency's clandestine tactics among its Western allies in the Transatlantic region. The National Security Agency's covert operations had came to world attention, through the media, when various tactics of mass surveillance had become public in June 2013. Which was consequentially followed by other revelations on later dates. The US had acknowledged there is much more information still in the hands of a former agent, which could lead to more international difficulties. In the process of researching and writing this thesis, the author conducted a literature search and reviews internal documents, literature reviews, news articles etc. This thesis is in fulfillment for a graduate course on conflict analysis and resolution/conflict resolution and Mediterranean security.

INTRODUCTION

Espionage is one of the oldest professions in the world, which has undergone several progressions while continuing to maintain cutting edge tactics throughout the centuries. Though intelligence gathering has functioned as a separate craft, diplomacy and espionage have been a dual activity as well, which has served as a single function of statecraft for centuries. Despite the fact that in a little over a century espionage has developed into its own intelligence department, it is now an integral establishment in many states spanning across the globe.

Espionage has increasingly become an important area for conflict resolution because of the digital technology evolution, turning traditional spying into cyber espionage. In the past spies were considered successful when they retrieved a physical folder full of documents, but in today's digital age it is easy for a hundred thousand or more documents, to be acquired in days or even minutes. Governments, businesses and average citizens in every part of the world are all now subject to become exploited victims. Given the new technology age and its continued pioneering capabilities, it is important that we reexamine the counter effects of espionage. The research and analysis in this study is aimed at understanding, how has the National Security Agency's (NSA) controversial cyber espionage methods impacted the US' diplomacy with her western allies. In addition, I am curious to see if there are economic repercussions due to the

NSA's cyber tactics. Furthermore, I will examine if the level of the NSA's cyber espionage has crossed the threshold of acceptance in the world of espionage.

Espionage is the practice of using spies to obtain secret information about the plans and activities of a foreign government, military, political entity or a business competitor. Spying is considered by several as the second oldest profession, since its history was first recorded in the Bible, "The Old Testament names the twelve spies Moses sent to the land of Canaan" and "Delilah was a secret agent for the Philistines" (Knightly, 1986: pg. 83). Both missions were to gather information from a foreign advisory to further their nations cause by use of military means.

The US' Department of Defense defines espionage as "The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation". It is clear that the US does not except any foreign intelligence gathering or espionage to be conducted upon itself, but what is also apparent is the US does condone such practices it conducts on to other entities. But this statecrafts "Illegal but accepted" practices are shared by most nations, if not all. Such state tactics are illegal to perform if they are caught, but it is universally recognized that all states practice espionage.

US Ambassador Brian E. Carlson's (2013) article in the Public Diplomacy Council describes diplomacy as, The work between governments that help maintain positive relations amongst governments. The three core missions of the US' public diplomacy are (I) Presenting and explaining American values, ideas and culture, (II)

Advocating U.S. policies, and (III) Shaping the foreign atmosphere so American objectives can be achieved.

When looking for where diplomacy and espionage served as a single state activity that function under one position, one could look to the American revolutionary War. During the War of Independence diplomats functioned as spies to undermine the enemy capabilities. Benjamin Franklin is one of the most notable Americans during the war who's acts of espionage and diplomacy helped the Americans win their independence. Franklin was a member of the "Committee of Secret Correspondence" which congress had sent to France in 1776. "Where he established a secret espionage ring of operation which allowed him to begin gathering intelligence and serve as a hub for the information network, while strengthening French support for the American causes" (Hastedt, 2011 pg. 310).

As technology had continued to advance throughout the centuries the dual edge of diplomacy and espionage had waned. Espionage in World War I had started moving away into its own separate entity starting with the British. Which "Formally created a British National Intelligence Service in 1909" (Srodes, 1999; pg. 53). After the British established the first intelligence agency many European countries followed suit in establishing their own. Buy it took the Americans over three decades before it would establish its own intelligence agency. In 1942, World War II was in full swing and President Roosevelt had commissioned the Office of Strategic Services (OSS). This was later to become the Central Intelligence Agency (CIA) in 1947, when America officially established its first separate intelligence entity. The CIA would continue to grow and

expand, its establishment in addition to its financial purse during the Cold War. Where it reached a level of grandeur with its competitor, the Soviet Union (Theoharis, 2011).

Since the end of the Cold War the level of technology in intelligence gathering field has reached farther, broader and deeper. Today, an individual's personal level of privacy and security are becoming less protected, which has sparked profound negative actions and sentiment globally. The digital age and cyber espionage have become the new standard across the world, mainly for the countries who have the finances and means to build such an infrastructure.

America, the number one economic power and military power, has been left in a precarious position. It's still having to deal with an ever evolving terror threat, in addition to other state actors and non-state actors digital technology advancements. Which have successfully breached the government, military and numerous private sector data banks. As the US continues to try and stay ahead of such adversaries technologically, many have asked if America has gone too far with its defensive tactics.

While there are separate intelligence and diplomatic departments today, we still can see where governments do have some overlapping between the two institutions. There are often cases when state representatives travel on diplomatic mission to a foreign state and deliberate intentions of espionage are conducted upon them or when a diplomatic station is used as a base of intelligence operations. All conscious minded states have procedures and protocol to guard against such activities, due to the common knowledge that all governments, if not most, spy. They have been spying for centuries, but the difference is the resources and capabilities they utilize today is unprecedented.

America has currently found itself on an international spectrum of conflicts. Diplomatically, it is currently having problems with some of its close allies in Europe.

Recent reports from 2013 and 2014 have stated the U.S. has conducted cyber espionage on allies such as France and Germany. Both countries have criticized the U.S. as an insecure ally who does not trust any of its friends, let alone their opinions of their own personal sovereignty being abused. Former French Prime Minister Dominique de Villepin stated, "America doesn't trust its allies," (Ing & Jamieson, 2013).

Reports come out in September 2013, that indicted the U.S. was spying on Brazil as well. Years of diplomatic efforts in strengthening the US, Brazilian relationship for a possible future alliance had been severally hampered. Later that month, the Brazilian President Rousseff used her time as the speaker at the United Nations to charge the United States of violating human rights and international law through espionage, which included spying on her.

In addition, other news reports came out against the US stating the government had spied on 70 million phone calls in France from the beginning of December 2012 to early January 2013. The broad degree of cyber espionage was reported to have monitored terror suspects, businesses and government officials. French President Hollande had came out and condemned the United States' spying tactics involving its allies (Payne & Shah, 2013). Furthermore, in October 2013 the US was exposed again for spying on another European ally. Reports had indicated the US had been spying on German Chancellor Merkel since 2010 and how her cell phone had also been tapped. Merkel later addressed

the issue and expressed how the US espionage had reached a new low and was becoming a serious threat to the Trans-Atlantic partnership.

With a continued barrage of news reports that the US had conducted cyber espionage from the highest levels of governments to the everyday average citizens, Germany and Brazil had presented a draft resolution in November of 2013 at the United Nations General Assembly. They had called for an end to excessive electronic surveillance, electronic data collection and other gross incursions of privacy. A discussion had begun about an international law that would limit the capabilities of cyber espionage.

Given the modern technology age and its continued pioneering capabilities, it is important that we reexamine what espionage is in the modern world and the affects of cyber espionage. On one side, espionage can strengthen alliances through shared information and on the other it side it can create or strengthen the friction of conflict between states. This study will center on espionage, its modern advancements and how it continues to be an important topic area for conflict resolution. The purpose is aimed at understanding how has the National Security Agency's controversial cyber espionage impacted the US diplomatically with her western allies. The research and analysis of this dissertation is to examine if the tradition of the universal acceptance for espionage can still work in the modern times of cyber espionage. In addition, it will examine if the level of the NSA's cyber espionage has crossed the threshold of acceptance in the world of espionage. In the following pages I will ask and answer the following questions. First,

how has the US' evolution of espionage tactics affected its Trans-Atlantic allies? Secondly, it will examine what are the economic repercussions from the NSA's programs? Third the research will look into what legal consequences has the NSA's digital spying programs motivated with her western allies?

LITERATURE REVIEW

Introduction

Based on the extensiveness of the study combined with the need to ensure validity and reliability, this literature review is based upon thorough research. This involves examining and extensively analyzing some of the secondary sources with reliable information on variables under the analysis, while seeking to offer a clear insight on the problems of cyber espionage and the current conflicts with the NSA under this research. The essence of this literature review is diverse based on the varying entities attached to the essential information gathered from the respective sources. The literature review involves examining some of the varying approaches enacted by the researchers, scholars and building on them towards offering more effective approaches to be used in the study towards ensuring validity and reliability on the information generated.

This is also essential towards examining some of the theories created or embraced by other researchers in relation to the issue or the variables under the study. Such theories are necessary in developing a detailed theoretical and conceptual framework under which the study is based to review the overall analysis. This is also essential for ensuring that the respective gaps that varying studies have failed to explore, therefore building on them towards offering a more reliable tool is achieved. Based on some of the statistics of research conducted in examining cyber espionage, the United States emerges as the

largest source in acquiring such information without any consumer or company consent. The NSA is one of the leading bodies that have admitted in using information from companies towards their operational goals solely based upon security. This has large implications for the country, despite the endless efforts and measures that the government and other security agencies are enacting with an aim of reducing such activities. While other nations view the US as conducting the same activities that US is advocating against. However, the implications and the damages caused by these activities affect not only the economic implications but also diplomacy on regional levels.

Furthermore, one of the major concerns that the respective players are currently witnessing is an inability of protection. They are prone to threat with cyber espionage with wide ranging implication of possible damages. In addition they have not discovered the historical aspect of espionage. Espionage has been there for numerous years used by nations such as the Philistines, Greece, and others to spy on their enemies especially during war. The implications of these activities have been social conflicts as some of these activities violate the civil rights causing numerous implications to the society. Lack of legal and restrictive international policies have largely attributed to the gradual growth and change of espionage over the years to the currently witnessed cyber espionage (Berkowitz, 2000).

The gradual development of espionage it has taken different forms, consequently providing an intriguing thought on whether the change in the development of policies prior to the current status quo could have aided the respective nations to avert the currently experienced damages. The assessment embraced under the stipulated concept

questions these activities, while also attributing the social conflicts attached to these actions. Merged with the failure of the respective stakeholders inactions to enact strategies and policies aimed at governing these activities. This could have greatly lessened the current damages experienced while also setting international policies and laws that could be governing the existing cyber espionage activities. The preceding analysis offers a historical perspective of espionage in relation to cyber espionage while also seeking to examine the respective implications on social and state conflicts. The study indicates the historical aspect of espionage and how it has gradually developed to the current form of cyber espionage while also examining the respective implications on societal clashes, state conflict and economic repercussions.

Espionage

Under the historical aspect, espionage is defined as the secret gathering of information based on the intentions and also the capabilities of other persons, organizations, groups, or even states. Espionage largely defers from intelligence based on the fact that intelligence entails gathering of information through broad means that is, either openly or secretly or the use of espionage jargon or even covertly (Hulnick, 1999). On the other hand, espionage entails to covert ways of gathering information that is, it is always conducted in secret. The attached analogy to the specific argument by the researcher depicts how espionage means the same as spying or even a clandestine operation which involves ground activity that cannot be easily tracked back to its source. Based on the stipulated analysis, as the researcher argues, it is evident that espionage or

spying has been part of the society for centuries. The assumption underneath the fixed notion reflects that spies have been constantly in use in historical and other forms of writings such as the bible.

According to (Gannon, 2001), there are two major categories of espionage activities or work. They are; HUMINT, or human intelligence where spies, agents are used, and SIGINT, signal intelligence that entails to codes, ciphers, secrete writings, secret monitoring of adversary's communication and also secret forms of communication. Based on the two stipulated forms or categories of espionage activities, it is apparent that SIGINT is the currently most used espionage with cyber espionage being the core entity in respective aspect (Miller, 1999). The definition of espionage and intelligence have received diverse aspects based on different researcher's arguments. According to some of these researchers, knowledge is commonly termed as power, the raw intelligence is not termed as power. The concept underpinning the specific relationship indicates that it is not enough to gather raw intelligence, without further information being explored, analyzed and processed.

The assumption encompassed under the specific aspects indicates that inherent to espionage, it is not only information gathering but also its analysis with the presentation passed down the chain of command and to other departments. Whether it is to military division or political committee or even economic leaders whom normally seem to adjust and adapt their own policies or tactics to align with the espionage concept. The research argues that there are four intrinsic steps that have been constantly used to gather and utilize espionage intelligence. They are; raw intelligence, processes intelligence, analysis

and policy outcomes. The stipulated analysis offers a clear insight on the integrated entities that defines the concept of espionage and its development of the currently popular cyber espionage. The notion given by the researcher indicates other players using the information for political, economic or military based implications argues on the intriguing implications on social conflicts as well as regional based entities which have emerged from these activities.

Why Nations Engage Into Espionage

One of the major intriguing analogies attached to espionage revolves around the main reason where it examines why states, nations or groups have been engaging themselves in espionage. In the histological and currently based aspects, the question on the essence of engaging in espionage has received diverse views from different parties within the international community. According to some of the researchers, espionage has been used by specialists, militaries and political leaders with an aim of reinforcing their decisions and judgments, hence the essence of espionage in the modern world. Some of the masterminds of the Golden Age of the Soviet illegal spy networks that were evident during the Stalin era in the 1930s, such as Alexander Orlov, indicated that "The essence of intelligence services in the fortune of nations cannot be over stated….the existence or the absence of a well working spy network on the territory of a potential enemy may spell the difference between victory and defeat" (Miller, 1999).

The same notion is attached to the comments availed by the Scholar Michael Handel who indicated the intelligence espionage is basically acts as a force multiplier

through facilitating a more focused and more economical use of force. The scholar on the other hand warns that when all the things are equal, poor intelligence is likely to act as a force divider through wasting and eroding strength. Under the long run, the parallel specified by the researcher indicates that the group with the better intelligence, is not only to use its power more profitably but also more effectively therefore conserving the concept and information generated (Hulnick, 1999).

Based on the analysis, it is evident that a numerous amount of these researchers tend to depict that there are some benefits with the use of espionage activities which can be traced back years ago. The concept and the approach derived from the given assessment indicates that states, organizations and different groups have been embracing espionage activities as a significant function that defines different aspects within the state and society. Given the availed analysis on the trend, definition and espionage activities, although vital to defining the study based variables, there are different gaps that exist in relation to examining effectively the variables of the study. These gaps include; whether organizations or the international community has enacted strategic approaches to govern such activities. Analysis on the literature above indicates that there has been minimal or no regulatory or legal based approaches enacted on the historical based era in relation to governing espionage activities.

On the global scene, it is apparent that espionage can change the balance of power among different states. The same approach could be traced on historical times as some of the nations with the most effective espionage tactics were considered powerful compared to those with the weak strategies (Hulnick, 1999). Nations such as China and Russia,

among others have largely been involved in such activities causing substantial losses and conflicts within the society, based on the economic and political implications involved (Cooley, 2002). In addition the US has also been blamed for such activities through the NSA's various operational programs. Even close Trans-Atlantic allies have fallen under some of the NSA's various cyber espionage activities.

One of the intriguing correspondences that can be traced from the detailed case depicts that offensive cyber capabilities are not likely to deter or even prevent cyber espionage activities. As discussed before, espionage is not a new activity and this can also be reflected on cyberspace, which has also been there for decades. This can be traced back in 1982; under which case a remote penetration of an opponent's computer network with an aim of extracting data through the use of internet could be attached (Cooley, 2002). Based on the notion that an operational goal of espionage is to perform undetected, with the cases when it is detected tactics are used to confuse observers while maintaining the general goal of remaining a secret. Everyone should not be surprised by the general low level of discussions available under the cyber espionage topic. According to Stephen Miller (1999), digital intelligence gathering is one of the most effective ways of espionage, based on the fact that the internet has produced a golden age for intelligence collection. Plus it has even brought the focus of conflict towards the gaining of the critical knowledge of an opponent's intentions and capabilities.

Trace evidence and analysis on cyber espionage offers a challenge to cyber security based on the fact that the current developments of offensive tactics seem too honed, expansive and largely on the rise. The fact that international laws provides little

recourse, the practice among the different countries has been to discreetly diverge and continue to overlook such discussions on the topic of espionage. The current outcome is similar to the situations before where no country has effectively been enthusiastically involved to embrace the respective changes (Hulnick, 1999). For instance, it is evident that the United States echoes that nations are going to indulge into espionage activities especially on cyber espionage. Though questions still remain within the global community on the form of the international framework that needs to be enacted towards managing and restraining these activities of espionage. Reaching a global consensus sooner rather than later is desired before such activities reach intolerable and potentially dangerous levels.

Some of these nations such as China are currently using cyber espionage as a strategic tool. They are using it to illegally access the United States' economic and military technology at unprecedented levels, with immense value of the intellectual property acquired by various nations, cyber espionage continues to prove as an intriguing parallel (Hulnick, 1999). Failure of nations such as the United States to effectively protect and safeguard their networks and also in failing to restrict its own espionage activities, continues to provide a lack incentives to stop other nations from practicing similar behavior. A continued practice of one country conducting cyber espionage activities and condemning other nations creates an environment which causes conflicts within the global society.

According to Berkowitz (2000), cyber espionage activities have increased over the last few decades due to the failure of enacting strategic approaches to govern and

restrict such activities. Which has lead to the high growth and a continued escalation of usage, while new forms of attacks are innovated on daily basis. The amended assessment on the specified analysis indicates that if strategic measures could have been enacted to govern and limit any form of espionage, the current social conflicts emerging through the increased use of cyber espionage could have been averted. Currently, based on the recent development and the use of cyber espionage, the only effective way to manage cyber espionage is through creating consequences in which they do not involve the threat of military response based on the fact that the threat is not credible. This is in part because presently the number of states conducting cyber espionage are too numerous, it is common for the perpetrator to be an ally and or often the victimized state is also responsible for similar activities.

The leading threats not only cut across different states but also on companies that are currently experiencing, loss of sensitive information, of customers, or strategies. All which can reflect decisive losses to an organization. If such cases occur across different regions, economic conflicts and social conflicts are likely to occur. Loss of sensitive government information on policies and security systems, or that of customers as experienced lately, by some of the leading global corporations has caused increased concerns reflecting costly losses to the respective companies (Lowenthal, 2000). These organizations are not only suffering key losses from the consumers, but also damages on reputation with the customers who are likely to pursue legal solutions especially when such information is used against customers without consent. These cases have been on the rise in the United States with broader and regional implications rising due to digital

hacking where organizations or agencies have acquired information from other nations' organizations without consent (Lowenthal, 2000).

Competitors acquiring sensitive information of a given company also reflects fundamental losses to the company. This is based on the fact that such companies suffering such a loss are not able to create a competitive advantage within the market with their strategies used by the competitors to gain the competitive edge. A lack of strategies or initiatives to validate, secure and produce policies to govern and limit such activities, have caused considerable losses and rippled into the economy.

Stock market manipulations also forms one of the global implications that companies are forced to avert. Such cases are likely to have considerable losses to the global economy and affecting nations worldwide, with possible conflicts likely to be experienced as people within the society demonstrate against such actions. The NSA's use of information from some of these companies without their consent is likely to have massive losses, as the affected organizations lose sensitive information to the competitors, while also damaging consumers trust and royalty. This reflects economic conflicts to the company involved and to the nation in general. Similar approaches embraced by the NSA are also being used by several nations to gather knowledge over other nations on security based information. The intelligence gathered has potentially significant implications on the victim nation.

According to the arguments presented by Gannon (2001), conflicts likely to emerge from cyber espionage ranges from economic, political and social conflicts, hence the essence of understanding the need for strategic policies limiting these activities. The

researcher argues that there is need to understand signals of intelligence based on the critical need for a coherent discussion of cyber security. The implications on such cases on espionage can be traced back in 1912, when Marconi invented the radio. Which attracted attention from various navies, in which they consequently had adopted it. However, after implementation the navies were not only able to effectively coordinate their far-flung fleets, but they also noticed that they had received other fleets signals apart from their own. Which allowed the new form of intelligence gathering to be accessible by anyone and it was also very likely to be unencrypted (Gannon, 2001).

The implication of the stipulated lesson from the invention of the radio on the early days depicts that intelligence opponents are able to quickly examine and exploit some of the technological vulnerabilities, plus the commercial technology, which proved to garner an inadequate ability to repel professional intelligence services. The same parallel can be traced where the militaries quickly learned, that anything which could be transmitted over the radio in a clear manner was an opportunity for their opponent, for this reason they resorted to encrypt their signals (Hulnick, 1999). The notion attached to encrypting a device involves plain text and then using them to turn it into given sequence of letters. that an individual without the key could not be able to access. This provided a situation where the individuals were seeking to encrypt the radio not only to intercept the message but also be able to crack the code set.

The outcomes made encryption harder to decode and also tougher to identify when it is not working. However, the United States was able to break the Japanese code at Washington Naval Conference which provided its negotiators with Japan’s internal

communications on their negotiating strategy (Cooley, 2002). The lesson that can be derived from such a case is that nations should not assume that they are safe, based on the likeliness for unpleasant surprises, without viewing the opponent's activity. The statement reinforcing the analysis explains how nations have been under effortless encounters aimed at breaking encrypted codes to access information from given states.

This can be traced back to a pivotal moment during World War II where incidents involving nations such as Germany, with their famous Enigma machine and Poland along with the British who developed Ultra, aimed at breaking the Germans code. The code breaking continued every night based on the fact that Germans made new encryption patterns every night (Gannon, 2001). The suppositions attached to the stipulated notion on espionage indicate how nations have been involving themselves in such intelligence gathering practices for decades. With minimal international policies to limit or regulate such activities. Thus, largely facilitating their usage across nations. The Enigma experience brings to the forefront numerous lessons in which a state can learn from and how to use resources affectively. Such as the human agents, ships, scientists, and currently satellites. State actors can utilize such information towards achieving intelligence success in the creation of their own wide range of intelligence capabilities.

Gaining access and control to the opponent's network has continuously been the pattern for cyber espionage (Hulnick, 1999). The concept attached to the illustrated case indicates that nation's current efforts to strengthen their cyber espionage activities is propelled by ill motives which are likely to reflect moderate to acute implications on different conflicts within the society. Currently, the commonly used technique is phishing

that entails innocent looking email which more often spoofs the email address and appearance of a friend or other associated entities and contains a document or a link which when opened it implants a virus or a malicious software on the network. Infecting the external devices such as Smartphone's camera or a thumb drive are also a commonly used technique today (Hulnick, 1999).

Later when the user is able to plug in or use the respective device, the malicious software is able to implant itself on the network. The attackers using these techniques are able to conduct reconfiguring procedures which allows them to discover and exploit flaws on commonly used software. This allows the perpetrators to gain unregulated access to the system later. Some countries are also integrating different entities such as cyber tactics, actions by human spies and some traditional signal intelligence, therefore creating successful operations (Jeffreys-Jones, 2002). The complexity of these operations are difficult to administer based on the fact that software continues to improve on its security. Which makes it harder for the attackers to access, though more advanced services and techniques are being developed. Consequently, it becomes harder to detect. The correlation attached to such cases include instances where the nations are not able to track or even prevent cyber espionage activities, forcing them to develop more complex systems to be able to achieve success in prevention and tracking of their adversaries.

There are diverse implications attached to the conflicts that are currently emerging based on the usage of cyber espionage. Some implications include conflicts similar to those expressed across different regions such as Germany and Brazil accusing the NSA or United States for spying on them. While on the other hand the United States

accuses China for utilizing cyber espionage activities against them (Berkowitz, 2000). The likelihood of more conflicts in the future can be traced to the increased use of cyber espionage, not only for economic based reasons but also on other areas such a theft of military technology.

For instance, Russian cyber espionage efforts have been aligned on focusing less on economic espionage, but more on traditional military concerns and politically based issues. For instance, to probe NATO networks based on military plans (Jeffreys-Jones, 2002). These efforts and patterns run parallel with the larger international actions. Which are based on the lack of constraints to digital intelligence gathering, in addition to the decline of the detection ability. The implications emerging from actions executed by Russia and from other nations such as Iran stipulates the potential conflicts likely to emerge (Berkowitz, 2000).

Economic and political conflicts are some of the major quarrels experienced by various nations and companies due to cyber espionage. Such activities have lead to significant implications which has caused companies huge losses, as they lose their trust with their global customers and potential future customers. When the NSA or other institutions create a backdoor into several national and international corporations, privacy concerns on the individual level and multinational corporate level begin to feel adverse security and monetary affects. In addition, intellectual property and other confidential business information are also exposed. Security breaches attached to some of these activities are making organizations vulnerable to loosing information to competitors or

other players within the industry and also in the government based organizations (Jeffreys-Jones, 2002).

This not only causes huge losses, but also the reputation of the companies involved are also leading to conflicts across state borders. Such cases are likely to increase if no respective measures are enacted. Based on some of the studies conducted, the United States is a leading region where firms are affected by cyber espionage activities. The fact that the United States is one of the major sources of information gathering, there has been a change of perceptions with some of the nations in transatlantic region. Differing views have been brought to the forefront of the US with conflicts on political and economic based entities experience (Shulsky, 2002). They view the nation as a major contributor with its efforts failing to curb the global activity. The notion that this information is normally leaked by some of the agencies or trusted organizations presents an intriguing perspective on the complexity of how to effectively rein in the extensive and invasive use of cyber espionage.

Although the US government has developed measures with an aim to change the NSA's tactics with its allies in concern. The perception of these regional policies and the damages are diverse. There is a continued dispersion with various possible implications, that are likely to have considerable effects to regions and to the world (Jeffreys-Jones, 2002). Based on such losses, companies may not be willing to venture into the United States and its private sector. In an effort to avoid exposure of confidential information related to the consumers. The notion portrayed by the NSA is that it is monitoring and

recording conversations from people within the society without their consent. This has had large implications on United States and US corporations.

Cyber espionage and other cybercrimes, cost the world hundreds of millions of dollars every year, especially the US, which are likely to cause conflicts on economic and political issues (Berkowitz, 2000). Berkowitz indicates that the research analysis above, translates into over $100 billion of loss annually with the research and development expenditure. Which is largely increasing in value. These losses are causing regional and global economic downfall. Companies are threatened by the increasing number on electronic breaches with some of them failing to venture or enter into agreements based on such threats. The costs is not only translated through some of these activities directly but also with repercussions on employment opportunities. This is further compounded by the fact that as the US seeks to politically fight cyber espionage activities that are targeted against itself. While the NSA on the other hand is conducting the same activities causing massive losses on US's economy as companies fight to repair their damaged reputation on exposure of consumer information without their approval.

Although the above information is one of the major threats, it is evident that United States stands to lose due to their actions on invading companies globally in the name of security. The respective undertakings that the NSA has been taking is likely to cause hundreds of millions of dollars in losses in the US, especially through the lack of investments. In addition to a drop of sales on some of their global technology companies. The damage of reputation is attached to the incursion of a given company based on the NSA's surveillance. Research indicates that consumers purchase products and services

based on the company's reputation (Eisendrath, 2000). On the other hand, it seems that NSA's strategies are damaging the reputation of several companies in the United States, hence scaring away investors. The given correspondence indicates the possibility of the United States loosing on both ends, that is, based on the billions of dollars on cyber espionage and also on scaring away investors. This not only causes economic and political conflicts but also the possibility of more damaging conflicts in the near future.

Conclusion

Espionage as specified above can be traced back decades ago. The ancients also indulged themselves in espionage activities. Some of these ancient incidents include; espionage in the Old Testament, and Sun Tzu: Art of War among others (Gannon, 2001). Under each of the provided ancient cases, the respective individuals used espionage to convey and execute activities in an aim of ensuring that they achieve a set goals or objectives. Espionage or intelligence gathering has been a part of society for centuries, as addressed above. The use of surveillance has been gradually developing due to attributed and differing factors, such as cyberspace among other entities. Under the technological aspect, it has yielded the use of cyber espionage within the modern atmosphere as provided in the research. Over the years, as espionage has been developing, the respective social, economic and political conflicts have emerged within the everyday society (Shulsky, 2002). This depicts the essence and reasoning of developing resolution measures aimed at governing these activities, while ensuring that the conflicts emerging

from such cases are averted. The study seeks to examine such conflicts hence offering recommendations on the possible resolutions and policies that can be acted to minimize such incidents.

RESEARCH METHODOLOGY

Introduction

The dissertation addresses the issue of the NSA's cyber espionage use and its implications with the US and its Transatlantic allies. Through the study and use of a secondary research approach, which is done through the investigation of the existing data after research and collection, the analysis will be carried out by primary research methods. Information resources collected for my dissertation are through books, articles, printed journals and also online journals. Which will be employed to give validation on the academic research carried out, presented and in addition to support the topical arguments that are well discussed through the sections of the dissertation. For more updated data, the study uses websites obtained online and also their specific examples. The public books and the academic papers that have been included are to give clear knowledge of the topics of discussion.

The research incorporates effective data and information collection from sources that retain such data on, cyber espionage activities while advocating on conflicts emerging from such activities and how to resolve the emerging differences. The study integrates empirical evidence and strategies to ensure that the information collected is not bias. Furthermore it is also to verify that the information generated is within the range required. This is achieved through means developed during the collection and analysis of

the information. The selected sources of data incorporate diverse views from several selected criteria. This is to facilitate, promote and incorporate views and expressions based on the study. The outcomes will be based on achieving transparency and offering results based on the objective of the study. These results should be used to address the study on the current problems of the cyber espionage impact with the US and the Transatlantic allies, hence the effective and efficient data collection approaches used.

Research Approach

The deduction and the induction approaches have actually been in existence for several years and have also been developed by different movements and theories influence (Zhang & Wu 2010). Peter et al (2007) claimed that deduction is a mechanism whereby a theoretical and conceptual structure is purely developed and tested through process of observation empirically. The specific instances are obtained from the general influences existing. In induction the concept of hypothesis is first tested or simply created through the means of data analysis. However the deductive reasoning the person researching actually goes through, provides some general statements so as to reach the conclusion logically (Wilson, 2010). In the other way, the basic conclusion is actually developed from the general principle. Deduction is actually very consistent with the philosophy positivism. Collection of data and analyzing data is the first step of inductive approach. The following step is actually to derive a theory as the way of analysis. The inductive structure approach is more flexible than the approach of deductive, this actually

enables the researchers to facilitate changes as the process of research continues (Saunders et al, 2009).

The study is based on a qualitative approach where the data collected and findings presented align with the concept that underpins the qualitative method. The study seeks to utilize such entities, thus creating a more distinctive approach on cyber espionage activities in relation to impact on changing perceptions of US vis-a-vis the transatlantic regions and the respective conflicts or implications attached. Through examining the events on how cyber espionage has been unfolding for the last few years, the study seeks to offer a clear analysis on the respective implications

Procedures

The essence of this section is to depict how the data collection on this study is systematically executed, whereas to give the acceptable answers to the problems of the research and its objectives. There exist several main alternatives to research design and the archival. The case study will actually be adopted as the most consistent mechanism for this form of research due to the fact that the study requires the use of observations, research and investigations. Perry C. (1998) argued openly that the strategy of the case study basically involves the trial to examine the relationship, which exists in reality and are often found in the single forms of organization. The strategy of the case study may actually be either phenomenology or positivists in nature depending on the researcher's approach, the collected data and the employed analytical techniques.

As mentioned earlier these sources are credible and offer a diverse richness in reference to credentials required in the study to achieve the objectives. The procedure of collecting this data was by consulting with various organizations documents. Analysis and close scrutiny was developed to ensure that the documents selected from these organizations were valid, reliable and within the specifications of the study towards achieving the objectives. Scrutinizing and deeply selecting these sources was to ensure that the data collected was also up to date, related to the study and avoid bias sources. After analyzing and selecting these documents from the vetted reliable resources, the data was analyzed on basis of consulting the respective stakeholders on the effectiveness and reliability of these sources. To enhance efficiency on the selected data and the resource origin, the information collection procedure ensured comparisons through strategic process were enacted. The collections of the data procedures were essentially to enhance transparency, accountability and fairness.

Research Method

In this research, the study was carried out purposively to create a universal comparison which would clearly bring an unambiguous insight on conflicts emerging from cyber espionage activities based on the impact exerted. The study seeks to purposely use qualitative data collection and analysis technique based on the area of cyber espionage and conflict resolution while also ensuring that the data findings and presentation aligns with the area of the study.

Qualitative research is more tentative in nature based on the concepts and

approaches that underpins the technique. Qualitative researchers objective is to collect an in-depth understanding of human conduct and the causes that manage such conduct. The strength of this approach lies in the fact that it has as holistic focus, allowing for flexibility and the attainment of a deeper, more valid understanding of the subject than could be achieved through a more rigid approach (Gray, 1984). Margarete Kern (2009) argued the importance of creating new criteria for establishing academic rigor when adopting such method. Such standards are integrated in the study to enhance validity and reliability of the data collected and information generated.

This research uses qualitative methods towards effectively examining the variables of the study and also addressing the current US and Transatlantic problem. The underpinning concept on the conflict emerging from cyber espionage activities and the need to develop resolutions through different global and regional channels is one of the main analogies behind the use the specified method of research.

Validity

From the methodological perspective, validity is the success of a scale in measuring what it was set out to measure, so that differences in individual scores can be taken as representing true differences in characteristics under study. From that perspective therefore, the researcher consulted statistical specialists and the supervisor who ensured the relevance and suitability of the content in the analysis would provide coverage of the objectives of the study. This aligned with qualitative method embraced under this study.

Therefore, from the analysis of research work of Rolington (2013), the generalization of the right instrument as with validity require the derivative of the formula to be at bar with the required index. Thus for the instruments to be accepted as valid, the average content validity index should be under the set standards. Furthermore the contents of the instruments were valid and constituted the major derivatives of the research.

Reliability

This entails to the measure of the degree to which a research instrument yields consistent results after repeated trials. According to Rolington (2013), reliability refers to consistency and stability in measurements. To establish the reliability of the models used, the researcher used the methods of expert judgment and pre-test in order to test and improve the reliability. This study used the respective qualitative method approaches that align with the specified view. This was aimed at ensuring that the data collected and presented provides a significant tool that can be used in decision making and policy formulation to address conflicts and offer resolutions emerging from the continuous use of cyber espionage by different state actors with a focus on the US and its Transatlantic allies.

Measures

To ensure that the data collected was reliable and effective in reference to the credentials and objectives of the study, specific measures were developed. Some of these

measures that were developed in reference to the determined guidelines and policies include; ensuring that the data incorporated in the study had supportive credentials, was related and from reliable and valid resources, the organizations had minimal or limited influence on the outcomes of the study and the strategies and mechanisms' used to measure the data collected and presented were reliable and within the required baselines. Developing and ensuring that these measures were enacted and utilized during the study ensured that the resources and the information derived from this research are not only within the required specifications but also presentable and credible. Various researchers recommend developing this measures as the guidelines and the minimum operational ranges under which research is conducted. Stipulating these guidelines prior the collection or analyzing of data not only strengthens the foundation under which the study was built but also the credibility of the data collected.

These guidelines ensure that the data collected is not biased and is presented in relation to the stipulated collection models. Also in reference with the essentials projected by the study are in relation to the set standards. The research involves the collection of data that correlates with the set study objectives, while also addressing the conflict of the US' cyber espionage tactics. The required measures on limiting irrelevant variables from a significant entity have been undertaken, in relation to make certain information generated is reliable and valid. This association was also reflected on the data sources selection and the agencies selected in the research. The collection and presentation of the data was essentially provided under guidelines and specifications of academics relative to achieving the study objectives.

Control Variables

These are normally variables that are extraneous and require specific strategies to avert alternation on the results or the data collection process. Various researchers control these aspects in their research thus leading to the essentiality to consider them in the study. The other aspect controlled by the study is the issue on cyber espionage while addressing conflicts, is to examine and analyze variables related to the issue of research while also ensuring that the data presented aligns with the study objectives. The reliability and validity of the respective research sources were to make certain that the respective entities underpinning the study are achieved.

Though some of these aspects were considered on the selection of data process, their influence was not presented on the study upon the presentation of the data by the research. Controlling these variables was also to provide baselines which underlie the need to ensure efficiency and effectiveness of the data collected. The essentialities of these procedures were very significant for the study towards ensuring that the information generated can be used in policy formulation and effective decision makings. Based on the extensiveness of the research, controlling the stipulated variables among other entities is vital in relation to offering reliable and valid information addressing the US' current cyber espionage conflict.

Data and Case Selection

The first issues that the study seeks to address involve examining various forms of cyber espionage which exists and also their effects and the severity. This also entails examining the respective implications on conflicts emerging from such cases under the issue. In addition to some of the effective strategic approaches that have been enacted on solving or that can provide resolutions, that can be acted to define a more effective environment where such conflicts emerging from cyber espionage can be examined. The study also seeks to briefly identify and evaluate some incidences of cyber espionage that have occurred and the respective implication on conflicts emerging from such cases while also examining the potential damages from such conflicts.

After the analysis, this research will give some vital and relevant qualitative aspects from different sources involving the amount of cyber espionage the NSA has conducted. In addition to the trends of the attacks and the financial implications locally and globally due to their threats. Combined with the potential conflicts emerging from such activities cutting across the regional and global boundaries. This is vital, since it will enable us to show the magnitude and prevalence of the NSA's cyber espionage issues, which directly correlate to global actors with their absolute interests in having a secure cyber space. Additionally, the study seeks to demonstrates how vital it is to discover the adequate global response on cyber espionage which is the major aim of this thesis. This is also supplemented on examining whether such conflicts may escalate in the future, the implications and the dangers involved, plus also ensuring that more effective measures are recommended based on the study findings.

The essence of the specified approaches and strategies is to ensure that the set objectives of the study are achieved while also examining the diverse conflicts and the potential damages. Examining current international laws and policies in relation to addressing such conflicts and also effectiveness on the strategies that have been currently enacted are also some of the approaches that the study seeks to embrace. Based on the sensitivity of cyber espionage activities and the potential source of conflicts, especially on cases where military or political based issues are attached, the study gathers data on such cases thus recommending on the resolutions. In addition to other respective measures that can be enacted to reduce the set implications emerging from the respective conflicts.

Furthermore, the research seeks to investigate into the attempts of cyber security by the United Nation as a result of their international status in terms of global security. The analysis provided on the specific concept is to examine likely areas of conflicts or already existing areas on different angles, while also examining some of the resolutions that can be enacted to minimize such implications. Through using several forms of data, the study embraces qualitative methods and the attached concepts on the presentation and collection of data. While looking at the UN issues, the study seeks to mainly examine on the resolutions, the content of resolutions, statements and the work being done by UN agencies in relation to cyber espionage and the strategies being employed, while reflecting on the conflicts emerging from cyber espionage activities.

The study seeks to briefly outline the positions and the efforts in regards to controlling cyber espionage by various Trans-Atlantic state actors and organizations

globally. This is to be achieved through a detailed analysis aimed at stressing the need to take in hand the current and potential conflicts with a cyber espionage origin. While also bringing further points for the need of acquiring support for a unified global consensus on cyber security by international organizations. Thus reinforcing my mechanisms by examining the major factors which is hindering such types of treaties at the state level. Additionally, the study seeks to emphasize strategic approaches on resolutions to cyber espionage, such as building global security through binding international treaties. This is aimed at examining the United Nations since it can produce greater outcomes due to its international status and leverage. The concept underpinning the set assumption is based on the likelihood that they are liable to cause different forms of conflicts, therefore the need to enact measures of resolutions to avert damages on regional and or global scenes.

For instance the study seeks to examine different cases indicating how cyber espionage has been on a constant state of evolution without restrictive measures and policies hence causing conflicts. Such an instance can be portrayed on a case such as when Mandiant, a company involving cyber security shocked the world when they published a series of possible attacks that were aimed at American companies as well as agencies within the government. It specifically specified beforehand that the attack was being planned by the operation based in Shanghai that was known as the People's Liberation Army Unit 61398 and also their exact location in a building in Shanghai.

Mandiant was questioned whether it was a good decision to publish such sensitive matter. Their spokesman responded that they were compelled by the news since several organizations were expressing some signs of absolute frustration and small tolerance with

the situation involving the acquisition. Asked if it was a wise decision to publish this information; one of the trusted CEOs actually said that we are what we call the time bomb while someone goes publicly with the sensitive information. The accusations were denied by the Chinese defense minister hence setting a foundation for more attacks. The stipulated scenario reflects some of the conflicts likely to have marginal implications within the society if cyber espionage activities are not governed. The study collects data on such cases while examining conflicts, the resolutions that can be enacted while also examining whether the current efforts enacted by nations such as United States are effective in curbing these activities.

Conclusion

The study seeks to embrace qualitative method through gathering and collecting data from different sources. Such entities include examining data through sampling speeches, news sources and texts on cyber espionage and conflict between the respective involved parties. The study examines various forms of cyber espionage in USA and their friends from the west while also evaluating on the nations which have been actively taking these attacks to high level. Some of the primary data sources will consists of government documents, regional news agencies, international news and the national news. The information sources will offer information on the economic repercussions and the political issues while largely focusing on conflicts and the possible resolutions. The secondary sources used in the study include books, articles and peer review journals hence examining diplomatic stand on the relations and also statements on the issue of

cyber espionage to USA while examining the conflicts emerging and the possible resolutions that can be enacted.

CHAPTER 1

ESPIONAGE

Traditional Espionage

A state without capable spies, is a government that is left in the dark and often exposed. Espionage provides governments with a protective barrier against foreign threats and aggression, and many governments have used espionage against their adversaries since ancient times. As Knightly stated, it is the second oldest profession as it was recorded in the old testament (1986). Governments in the past spent considerable amounts of resources on their espionage operations and governments continue to do so today, but the amount of resources utilized to build and maintain the capabilities is drastically different. States expend numerous resources to build and maintain their capacity to spy at present. The amount of financial resources expended to espionage to obtain secret information about the plans and activities of a foreign government, military, political entity or a business competitor, has only continued to increase.

In the eighteenth century and well into the twentieth century is the traditional age of espionage where many individuals reflect back to cylinder container locked with a cipher which contained a secret manuscript or to a spy who has infiltrated state to gain access to secret documents. This was a period where spies were most common tasked to acquire an enemy's military whereabouts or some intelligence on a clandestine operation.

Some famous cases of military espionage included Major John Andre who spied for the British during the American revolution, he was later caught and hanged by the Americans. Germanys famous courtesan spy Mata Hari whose code name was H-21, who was captured and executed by France during World War I (Hastedt, 2011; Barboza & Drew, 2013). When thinking of espionage and recent secret agents many reflect back to the golden era of the CIA and the Komitet Gosudarstvennoy Bezopasnosti (KGB). One of the most significant cases of espionage was conducted by the Soviet Union where numerous KGB agents were involved in intelligence gathering operations against the West. When 1949 the Soviet Union detonated its own atomic bomb, this had caught the West completely off guard as most experts had not expected the Soviets to acquire such technological capabilities till years later (Lundestad, 2010).

Though spying is an ancient practice, spy agencies are relatively new. It was not until 1909, that the British Empire established the first intelligence agency as a government department. The agency's employees were largely citizens, it was financed through government resources, the agents were tasked to steal secrets from other countries and to protect its own state while it operated in peace as well as in war (Dulles, 1999; Knightley, 1983). Other European states followed shortly after, but it was not until 1942 during World War II that the United States established its own intelligence department, the Office of Strategic Service (OSS). Which President Roosevelt had used a presidential military order to create the organization. The intelligence institution had been tasked with collecting, analyzing, and dispersing the Axis' data to military and political leaders. Though the OSS was a US agency, it was in its early years of establishment, it

relied heavily on the British Empire for much needed assistance in intelligence gathering. Following the end of World War II the United States government overhauled its military and intelligence departments with the establishment of The National Security Act of 1947. President Truman elected and the senate confirmed James Forrestal as the first secretary of defense and the Central Intelligence Agency (CIA) was initiated in which it succeeded the Office of Strategic Services (Liptak, 2009.)

The National Security Agency (NSA) was established in 1952 by President Truman through a secret executive order, the National Security Council Intelligence Directive Number 6 titled "Communications Intelligence and Electronic Intelligence" and its institution was kept secret until 1957, where it was first mentioned in government documents (Weiner, 2008). The NSA was another intelligence agency the US had established for which it was charged with a specialization in global monitoring and information gathering through Signal Intelligence (SIGINT), where the director had been granted full power of control over all SIGINT collection and processing activities. The NSA is described as providing foreign Signals Intelligence to the nation's military and government policy makers, which gives the nation's leaders vital information that is needed to defend the US and advance its goals (Hastedt, 2011).

Subsequently the NSA falls under the United States Intelligence Community which was established in 1981 under President Ronald Reagan through the Executive Order 12333. The US Intelligence Community (IC) is in charge of seventeen different government agencies such as, the CIA, NSA, Department of State and Army Intelligence, that work separately in intelligence gathering activities that are deemed necessary. The

Director of National Intelligence (DNI) is the head of the IC and reports directly to the President. The US' Intelligence Community is charge of the world's largest intelligence agency which has command of an annual budget that is the size of a small countries GDP. The Director of National Intelligence had disclosed its aggregated amount of monetary funds, that Congress had appropriated to the National Intelligence Program (NIP), for the fiscal year of 2011 which had an aggregate amount of $54.6 billion (Office of the Director of National Intelligence, 2011).

Modern Espionage

Cyber espionage is the use and targeting of computers to obtain a secret of some sort. Much like other forms of espionage, it is clandestine and usually involves a government agency. This digital form of intelligence gathering dates at least to 1982, when Soviet KGB spies reputedly stole a Canadian firm’s software that had been laced with a logic bomb secretly planted by the CIA. It is in the twenty-first century, however, that digital espionage has truly taken off. Every intelligence agency in the world operates in this realm, and every country has been targeted. (Singer, 2013)

Since the last few decades of the twentieth century, the world has seen fiber optic cables and the internet connect the planet in such a way that it had only been imagined in science fiction. Now more than ever before is the world connected. Thomas Friedman (2007) even went as far as claiming "The World is Flat" and he wrote in his book on how globalization had created an international, level playing field. The importance of location and opportunity has become an almost obsolete apprehension. This is in a large part since

the development of the internet, telecommunication networks and the rapid growth of modern data. The world has never been linked with such intensity before. Our communal perception has permanently changed forever. Technologically today is interwoven so deeply in most of the world, that one could never simply pull the plug on an integrated nation. Most nations economies, infrastructure and military defense have come to rely on modern technologies connectivity. The growth of fiber optic cables with new software has increased the dependence of the everyday average person and governments with the personal computer. Companies like Google, Amazon and Cisco are heavily used and depended upon across the world. But where comes positive civil innovation also comes negative government exploitation. Just like the atomic bomb, a new race has begun.

Edward Snowden

The NSA describes itself as leading "The U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances" (The NSA/CSS Mission - NSA/CSS), and the world learned just how powerful some of the NSA's tools were capable of from documents leaked by NSA contractor Edward Snowden in 2013. Which had detailed how the US intelligence agencies and their allies engaged in online surveillance of an unprecedented scale. The approach was to monitor as much Internet traffic as possible, with a particular goal of collecting what is known as

"Metadata". Essentially data about the data itself, metadata is information that describes the nature of communication, rather than the content. In traditional telephone surveillance, for example, this would simply be a record of what phone number called another phone number at what time, as opposed to what was said on the call. In the cyber era, metadata is far more complicated and thus far more useful. It includes information about geographic location, time, e-mail addresses, and other technical details about the data being created or sent (Singer, 2013).

On June 5th 2013, the British news agency "The Guardian" revealed classified documents from the former NSA contractor Edward Snowden. They revealed a U.S. ostentatious cyber strategy intended to safe guard the US from terrorist attacks which had utilized programs derived from Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism US Patriot Act of 2001, and on Section 702 of the foreign intelligence surveillance act of 1978. The cyber security apparatus was strategic in providing grand cyber espionage tactics which had been applied in a global security context, during peacetime operations, on U.S. soil, with resources outside of the military's extent. Snowden worked for the NSA through the subcontractor Booz Allen in Hawaii. After three months of working there he became disturbed at what he had found. The NSA's large scale of domestic surveillance practices had frightened Snowden to the point that he began collecting such top secret documents pertaining to their surveillance activities. Snowden took the stolen top secret documents and fled to Hong Kong.

He approached the Washington Post, and the Guardian newspapers. They decided to print some of the disclosed information they had received on June 6th, 2013. Once these news agencies posted and printed the information, they went viral. Several other news agencies worldwide began printing, posting and airing the documents information. Many of them had detailed the invasive spying practices that the NSA was conducting against American citizens. There were three main spying operations that Snowden provided information on. They are PRISM, Xkeyscore, and Tempora.

The documents enclosed an enormous amount of damning information against the NSA's umbrella of domestic and foreign surveillance practices. First, it included information on the PRISM program, in which the government had been spying on millions of American citizens since 2007. PRISM allows an agent to conduct real time data collection. It is a surveillance operation that allows the NSA analyze, extract and capture information about consumer activities on cell phones and computers. Activities that have be known to be retrieved are such as, emails, photographs, audio and video chats, documents, as well as other materials. Sources of information have come from companies such as, Apple, Microsoft, Google and other Internet firms. An overflow of information had followed, leaving the international community and American citizens critically searching for more information. While the United States government have been devising on how to obtain Snowden. Edward was asked why he chose to leave his six figure income and expose the US secrets, he was quoted as saying, "I'm willing to sacrifice all of that because I can't in good conscience allow the U.S. government to

destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building" (Smith, 2013).

On July 31, 2013 Snowden spoke with the Guardian newspaper again and he exposed a second NSA surveillance program named "Xkeyscore". Which is another NSA top secret program that gives analysts the capabilities to search through vast databases containing browsing histories of millions of individuals, their online chats, social media activity, emails and metadata, without prior authorization. Though US politicians on the intelligence committee have denied such capabilities are attainable and Snowden is dishonest. But the training material he had provided on Xkeyscore detailed how NSA specialists use it to extract massive amounts of information from agency databases. An agent can easily justify his search through an on screen form that grants his request in which there are no courts involved. The program was also boasted as the most extensive data snooping attainment capability the department had in developing intelligence from the internet.

If an email or IP address is known by an analyst, such minimal identifying information provides the agent with enough information to obtain extensive electronic surveillance on US and foreign citizens without a need of a warrant. This system grants the power to nearly examine a limitless range of internet behavior. In addition it permits an agent to track an IP address that visits a website. In essence, the NSA has the opportunity to observe anything a common internet browser has done or does. Nearly one trillion cell phone and one and a half billion internet events were captured in 2007, one report suggested.

On June 21, 2013, the third surveillance program called Tempora was exposed. In 2008 Tempora was piloted in the UK as another electronic surveillance program. It was successful and permanently established in 2011. The Government Communications Headquarters (GCHQ) heads the program for the UK and the NSA runs the American portion. Data in fiber optic cables are intercepted, then the data is stored, and advanced computer systems sift through billions of electronic information searching for potential targets. Once again, personal information and data is collected from the internet, with the company owner of the cables or landing stations, having full awareness of the governments spying. Citizens and criminal targets are not divided from one another. GCHQ had probes attached to more than 200 internet links by Summer 2011, each probe carried 10 gigabits of data per second. There is current work on expanding their capabilities to 100 gigabits a second. The GCHQ and the NSA are only a small portion of the states involved. The other "Five Eyes" nations are also suspected of being involved. Five Eyes are the US, UK, Australia, New Zealand and Canada. These nations started their global surveillance organization since the cold war. The GCHQ was also stated as saying they are the top data collector of the group, and gathering more meta data than the US' NSA. (Ball, J. *et al*. 2013). Five Eyes has also been linked to several other western states which act as third parties. It is understood that the global surveillance group is not limited to just five countries, but it had grown into a partnership involving more than ten states.

US officials have admitted that only a small quantity of the roughly five hundred thousand classified documents have been revealed to the public. Obama officials have

said behind closed doors that Snowden possesses enough material to keep the media entertained for a couple of more years. Some of the information that has not been published contains government employee names. These government secret leaks have ignited several diplomatic cries of outrage with the US from its western allies. In addition, the US intelligence officials say they are trouble with a "Doomsday" cache of extremely classified documents which are in his possession (Hosenball, 2013). Though they are strongly encrypted, other nations have the skill levels to break through the protection which is stored on a data cloud.

International Reaction

The US State Department declares that the American mission of public diplomacy is to support the achievement of U.S. foreign policy goals and objectives, advance national interests, and enhance national security by informing and influencing foreign publics and by expanding and strengthening the relationship between the people and Government of the United States and citizens of the rest of the world (U.S. Department of State, 2014). Though the Snowden leaks had proffered an analogy between the US State Departments diplomatic operations and within the NSA's state security mission, hence, the occurring diplomatic conundrum the US is facing with it Transatlantic allies.

France had summoned the U.S. ambassador to talks on October 21, after Le Monde newspaper reported the NSA had been spying on French citizens on a massive scale. The NSA leak stated that it had recorded nearly 70 million French telephone activities from December 2012 to January 2013. The targets were to be suspected

individuals with connections to terrorism. But such large scale data collection acts like a vacuum and it sucked up everything. It had also revealed that information connected to people in French politics and businesses had fallen victims to the data collecting. French Foreign Minister Fabius had called the disclosures intolerable and Prime Minister Ayrault said he was deeply moved and shocked by these claims.

Both the French and US presidents reached out and contacted one another a few days later, so they could discuss the cyber snooping allegations. President Obama assured President Hollande that he is reviewing how the US surveillance and intelligence gathering is operated and conducted with its allies. The head of the Direction Centrale du Renseignement Intérieur (DCRI) intelligence service in 2012, Bernard Squarcini commented on the NSA report. France spies on the US just as the US spies on France, commenting on reports that the NSA recorded millions of French telephone calls. He stated, "I am amazed by such disconcerting naiveté", "You'd almost think our politicians don't bother to read the reports they get from the intelligence services." (Todd, T. 2013). Since October had passed, the French government had quit its rhetoric towards the US and it NSA allegations.

On September 9, 2013 the President Rousseff publicly spoke out against the US in regards to the newly uncovered NSA documents. President Rousseff had become aware that she and her country were spied on by the US. After she openly denounced the US and its cyber espionage practices, she highlighted that Brazilian sovereignty could have been violated. After the leaks exposed that the NSA spied on emails, phone calls and text messages of Pres. Rousseff, she cancelled her state visit to the US in October. At the end

of September the U.N. General Assembly took place. Pres. Rousseff was the opening speaker and she continued to rail against the US espionage tactics as a violation of human rights and a infringement on international law. She went even further as she recommended a framework for an international governing body to protect against cyber spying, proclaim Brazil was developing defensive technology and ratifying laws for self protection.

Late in October 2013, more damning NSA leaks had surfaced about the US. The US was using its embassy as a spy base. It was conducting surveillance on German citizens, businesses and on the government. More importantly it was performing cyber espionage on the German Chancellor Merkel for several years. On October 24th, Chancellor Merkel gave harsh words to the US in response to the disclosed NSA information by Snowden. She accused the United States of damaging the diplomatic relationship to an unacceptable level which had violated the alliances trust. The accusations blamed the NSA for her cell phone being tapped. Germany's foreign minister summoned the U.S. ambassador to Berlin to discuss the issue. This was an unprecedented diplomatic maneuver that has not been seen with the two states in the past 60 years. The roof of the US embassy in Germany that was used to monitor a large part of cell phone communication in the government quarter in Berlin has been at the heart of the problems and it had not gone away.

Reports had also indicated the US had been spying on German Chancellor Merkel since 2010 and her cell phone was also tapped. Merkel condoned the US cyber spying programs which she said have reached unprecedented levels. Which resulted in Merkel

backing out of the US and EU free trade agreement known as the Transatlantic Trade and Investment Partnership (TTIP). She wants new assurances and new agreements before the EU will talk with the US on restarting the discussions on the TTIP deal. Chancellor Merkel not only commented that the current data accords needed to be altered, but in the beginning of this month the Brazilian President and she had presented a draft resolution at the UN general assembly which called for an end to disproportionate electronic data and surveillance collection.

On November 26, 2103 at the United Nations building, the General Assembly passed a resolution. This was long a waited by the Brazilian President and the German Chancellor. Though the resolution is largely symbolic, it still sends a clear message to the US. While such resolutions are not bound by law, they do echo a world attitude towards an issue and it carries a lot of political clout. The adoption of the resolution is now likely to pass the 193-member General Assembly later this month. The resolution it focused on prospective threats to human rights, with a spotlight on the right to privacy in the modern digital era. Since the NSA's worldwide surveillance programs broke earlier this year in the summer, states have been frantic about their security. Stronger relationships have been forged in response to the US' cyber espionage, while the current alliances with the US have hit a cold spell.

“Through this resolution, the United Nations establishes, for the first time, that human rights should prevail irrespective of the medium and therefore need to be protected both offline and online,” replied a Brazilian representative (UN General Assembly Meeting, 2013).

Conclusion

When Snowden started to leak highly classified documents from the NSA during the summer of 2013, no one could have truly predicted what adverse repercussions were going to challenge the US. The proffered information of the US' metadata collection had proved that the NSA's digital surveillance was not of the old traditional espionage tactics. The NSA had been collecting billions of bits of data from its allies. Tens of millions of citizens had their personal information collected and sent back to the US. The continued exposure of the US governments unprecedented international digital espionage activities had proved to have considerable adverse effects, which has created a state of conflict between itself and its Transatlantic allies. The recent NSA revelations have exposed some of the most sophisticated data mining and collection operations, of metadata that has never been seen previously. The covert digital surveillance activities had siphoned and compromised information from the French and German states virtual communication systems on such broad and deep levels that data from everyday citizens, to corporations and even at the government echelon. The NSA had been caught on the border line of performing economic espionage, in regards to businesses and employee data being extracted. Though the NSA's response was such programs are only designed for targeting terrorists, which protects both the US and its allies from future attacks on their soil.

The US has lost its former level of trust with Transatlantic allies and it has a long road ahead of itself if it wants to begin repairing its relationships. For the US to resolve its conflict with is Transatlantic allies it will need to first begin with being more

transparent with its allies, in addition with coming forward with some of its other operations that may have not been exposed yet by Snowden's cache. It would better to get a head of the situation before the conflict has an opportunity to deepen. Second, the US needs to scale down the NSA's cyber espionage operations such as, PRISM, Tempora and Xkeyscore, considerably. In doing so, the US would show it acknowledges the severity of its actions, the damages, conflict it had caused with its Transatlantic allies and that it is serious in working with them to seek a resolution of positive peace. With transparency the US could prevent more diplomatic fallout, repair its image and resolve the current conflict (Greenwald, 2013).

CHAPTER 2

ECONOMIC FALLOUT

Introduction

Defined as the usage of computer networks towards gaining illicit access to confidential information mainly held by a government or other organization, cyber espionage reflects wide range of currently expected annual losses globally (Prodhan, 2013). This has reflected a growing concern over cyber espionage and the intellectual property (IP) theft, especially the trade secrets with an aim of reducing the respective implications or losses. Cyber based threats have been in existence for a long time accelerated by the rapid technological advances that has resulted to greater connectivity, data storage, increased globalized supply chains, has increased the opportunities, potentially payoff, and also breach of corporate networks and acquiring sensitive corporate data. Current technological developments and increased connectivity has reflected marginal changes on social, economically, and globally political aspects. However, the same technologies that have largely accelerated the global growth are currently being used to harm economies and propriety information.

The United States has been in the center of a global controversy after NSA spying portrayed as risking billions of dollars in US technology sales. The impact of cyber espionage reflects numerous negative implications. The decision by a congressional

committees on blacklisting Huawei Technologies Co. products from United States telecommunications market based on allegations on enabling China to spy on United States, presents a threat on economic development (Prodhan 2013). The same decision is being projected to also likely affect Silicon Valley. This is based on the report by the National Security Agency persuading some of United States based technology companies to develop what researcher's terms as backdoors on security through security products, devices, and networks hence allowing easier access and monitoring same with those described by the House Intelligence Committee as threat posed by China as reflected by Huawei. The implications on these cases China based Huawei is estimated to have business as companies in the US failed to use its equipment. Researchers estimate reduction on US technology sales in overseas by over $180 billion by 2016.

It is evident that the current allegations directed on NSA and United States government is having massive economic consequences. This is also reflected on the fact that implications are also beyond financial or reputation but also across borders, this is evident based on the allegations published German news agency Der Spiegel (Poitras, 2013) claiming that NSA had cracked encryption codes hence listening on to 1.4 billion smart phones globally including that of Apple Inc'.s iPhone. The chain of allegations by NSA invading some of these companies and using their information against their consent presents an intriguing analogy on effectiveness of dealing with security while ensuring trade secrets laws and regulations are safeguarded. Companies and organizations such as Google, Yahoo, and Facebook Inc. have been forced to petition United States Foreign Intelligence Surveillance Court that is mandated with on making ruling on warrants for

the domestic data towards offering them permission to publish the types of requests that they receives from NSA (Prodhan, 2013).

Companies such as Cisco on the other hand, have indicated that they don't customize equipment hence enabling surveillance. According to the report by some of the senior managers in the organization, they argue that their product development practices and policies doesn't advocate for international behaviors or product features that are designed allowing unauthorized devices or networks to access or expose sensitive device information. The company denied the claims that they were aware of NSA having an encryption program.

These undertakings United is likely to have massive economic implications based on study conducted by Rachael (2013). The researchers indicate that some of these undertakings being enacted by NSA are likely to kill United States technology industry. US technology industry largely depends highly on overseas market with some of the leading companies acquiring substantial shares of their revenues from the overseas markets. For instance Cisco System Inc. (CSCO), which is one of the leading networking equipment makers, recorded around 42 percent of its $46.1 billion in fiscal 2012 revenue outside the US. Symantec Corp. (SYMC) is also one of the biggest makers of computer based security software located in Mountain View, California that reported 46 percent of its fiscal 2013 revenue also outside US markets. Intel Corp. (INTC) reported 84 percent based on its $53.3 billion in fiscal 2012 also beyond US borders based on data collected by Bloomberg, Intel Corp. forms one of the largest semiconductor manufacturers in the world (Holmes, 2013).

According to Allan Holmes, (2013) these threats attached to cyber espionage among forms of cybercrime activities strikes directly at the core value of different corporations reflecting a core vulnerability likely to have marginal losses to businesses. The researcher also argues that trade secrets normally comprises an average of two thirds of the value of businesses' information portfolio, with researchers indicating that the percentage normally rises to 70 to 80 percent for the knowledge intensive industries such as the information service, manufacturing, scientific, technical services, and the professional services. The assumption depicted in the availed analysis above fails to address cases where some of the trade secrets made public becomes tenuous with their value not recoverable especially when acquired by the competitors. The fact that NSA and United States government is using such information with or without the firms consent presents massive economic implications on firms and United States in general.

The cyber espionage related intellectual property lost aggregate amount has been staggering annually. This is based on different factors within the industry with nations pointing figures on some of the major players towards enabling accelerating accessibility of information and the usage. This has created a vulnerable environment between firms and nations across the globe. According to the United States Department of Defense, every year, a large amount of intellectual property, that is larger compared to that retained in the Library of Congress, is normally stolen from various networks that are maintained by United States; businesses, universalities, plus different governments departments and agencies.

The same arguments can be reflected by a 2012 speech given by General Keith Alexander of the National Security Agency and U.S Command, who indicated that IP or intellectual property theft due to cyber espionage terming it the "greatest transfer of wealth in history", he also indicated that United States based companies annually lose over $250 billion due to Intellectual Property theft (Rogin, 2012). The problem is not basically limited to cyber espionage as trade secret theft continues to grow in different forms with integrating current United States with other entities recording over $300 billion. Historical trend on the growth of these cyber related theft and crimes are evident based on the fact that in United States the federal cases related to the trade secret theft were recorded to have doubled between 1988 and 1995, the same notion was also recorded between 1955 and 2004, with projections made of doubling again by 2017.

Although the availed analysis indicates the losses caused on firms and global economy due to accessibility of the information by these attackers, the fact that the NSA is also accessing such information or instructing companies to develop products to facilitate surveillance without consumers consent presents an intriguing analogy. Consumers are shunning away from organizations that have been involved in such cases causing massive losses. The same implications are reflected on regional base where countries such as in European Union are diverting their reliance on US technology assistance. This is likely to have massive implications on the nation's economy through not only scaring away consumers on some of the suspected products but also investors across these regions. The US seems to only address on cyber espionage caused by

privatized attackers on companies and government agencies while on the other hand, they seems to exercise the same activities.

The parallel stipulated indicates that the issue is larger than just a concern for the United States on cyber espionage related implications. This is based on the fact that economic espionage emanating from digital spying and trade secret theft is being practiced across different countries around the globe. This affects vast companies worldwide with nations accusing each other based on the highest players. The findings based on the data collected fails to be consistent with the United Kingdom having a significant increase on trade secret cases rising in Europe also recorded. Based on a survey conducted by European Commission, it depicts significant scope to the problem especially in the recent 10 years.

The study interviewed different respondents with five of those interviewed indicating that they have experienced at least one attempt or act of misappropriation within the European Union countries with around 40 percent of the respondents believing that the risk has increased in the same duration. The same analogy is reflected in the findings on a study conducted by the Japanese government that indicated that 35 percent of the respondents manufacturing firms have constantly recorded technology loss. Between 2004 and 2008 in South Korea, the implications from cyber espionage on the economy had tripled.

Although the availed analysis offers a clear insight on the need to embrace strategies aimed at reducing some of the cyber related crimes while also averting spying from some of the nations, it is evident that the economic consequences may largely affect

nations, especially the United States. Reports that the NSA had cracked protected emails, coded web content, and in addition to convincing some of the equipment and device manufactures to build backdoors into the products has brought questions to such digital security efforts. This is further worsened by the increasing allegations that NSA had been obtaining and analyzing communications from phone companies and also from internet providers.

The outcome of the US' efforts to protect their borders, and with an emphasis on security, especially on cyber based crimes presents an intriguing parallel as it tends to exercise the same activities. The revelations on these allegations have made the overseas governments question on whether they can be able to rely on United States technology. This is evident in transatlantic region where Germany has called for strategic measures against some foreign companies and to investigate where their privacy laws may have been violated. Germany's government has also called on the need for a homegrown internet, while advising email companies to investigate such claims, and a US southern neighbor Brazil has also suggested an investigation on whether foreign companies had violated privacy laws.

The notion embedded on the availed analysis indicates the possibility of United States recording massive losses, especially if nations such as the transatlantic based countries fail to use products generated from or manufactured in US. Companies in the US are already experiencing effects where nations such as India have threatened banning Google Inc. emails services in addition to Yahoo, based on a Wall Street Journal report

(Rachael, 2013), and in China the tension is evident with China Daily once labeling the United States based companies such as Cisco as a “Terrible security threat”.

In 2013, a study was conducted by Verizon Data Breach where the investigation report tracked six hundred twenty one breaches and confirmed that data which had been breached in the preceding year, ninety two percent of which, were conducted by outside foreign entities (Camille, 2013). The report also indicated that nineteen percent of these breaches were largely attributed to state attached actors, with the Chinese state affiliated actors contributing close to one fifth of all the breaches, with ninety six percent of all espionage related breaches (Camille, 2013). The study also specified on some of the common state sponsored forms of espionage which normally involves the usage of what the study terms as “Social tactics”, they include; spear phishing, and the percentage of the breaches through the use of social tactics being four times higher in 2012 compared to 2011, therefore contributing to twenty nine percent of all the breaches in 2012. Hacking also attributes to these breaches recording fifty two percent and forty percent from the malware. The availed findings are further supported by a study projecting the possibility of the largest global organizations facing an average of $35 million in losses (Camille, 2013) where in the next two year period they are likely to see breaches that involve attacks on cryptographic keys plus the digital certificates.

There has been an increasing concern on the need for the respective key players to develop strategic approaches aimed at governing and reducing such cases, the efforts have not yielded significant changes. These efforts can be traced from the government to the private sector as they seek to trace the origin of the attacks through improvement,

attributing attacks to specific perpetrators and also determining whether the perpetrators are state sponsored hence remaining a challenge as one of the technical matter.

The preceding study offers a detailed analysis aimed at examining the impact of cyber espionage towards changing the perceptions with the US vis-à-vis the Transatlantic and the economic implications. The economic fallout attached to the impact of cyber espionage is also one of the major objectives that the study seeks to examine. Through the detailed analysis on the stipulated entities, the study seeks to offer some of the most effective initiatives that can be enacted to minimize the impact on United States perceptions with Transatlantic countries and economic fallout.

Economic Impact of Cyber Espionage on US in Relation to Transatlantic

Based on some of the statistics of the study conducted in examining cyber espionage, the United States emerges as the largest source of acquiring such information without consumers or company's consent. The NSA is one of the leading bodies that have admitted using information from companies towards their personal usage especially security based. This has large implications for the country despite the endless efforts and measures that the government and other security agencies are enacting with a goal aimed of reducing the vice while nations view the US as conducting the same activities that they are advocating against. However, the implications and the damages caused by these activities affect not only the economic implications but also the regional bases. According to Sanger & Smale (2013) there are different components that can be sourced from cyber espionage. These parts are:

The Loss of Intellectual Property and the Business Confidential Information

This is one of the leading implications of cyber espionage which is causing companies huge losses as they lose their intellectual property and the business' lose confidential information. Security breaches attached to some of these activities are making organizations vulnerable to losing information to competitors or other players within the industry. This not only causes the huge losses but also the reputation. Based on some of the study conducted, United States is the leading region where firms are affected by these activities with the vice spreading across the globe. The outcome is a cost to the United States firms but to the global economy which can be measured in hundreds of billions of dollars. This is evident based on the current study by World Bank indicating that the global GDP was around $70 trillion by year 2011 (Jabeen, 2013).

The study also depicted a $400 billion loss on the high end of the projected highly profitable costs representing only a fraction of the global income. The fact that United States is one of the major sources of information, there has been a change on perceptions with some of the nations in transatlantic region having different perceptions on the nation. They view the nation as the major contributor with their efforts failing to curb the vice. The notion that this information is normally leaked by some of the agencies or trusted organizations presents an intriguing analogy on how to effectively curb the vice. Although the government has developed measures with an aim to change the perception on these regional policies, the damages are diverse and spreading with possible diverse implications likely to have marginal effects to the regions and the world in general.

Based on such losses, companies may not be willing to venture into United States to avoid exposure on confidential information related to the consumers. The notion portrayed by the NSA is that it is monitoring and recording conversations from people within the society without their consent. This is having large implications on United States.

Cyber Espionage and Other Cybercrimes, Costs the World Hundreds of Millions of Dollars Every Year

This translates to the availed analysis above indicating over $100 billion annually with the research and development expenditure largely increasing the value. These losses are causing regional and global economic downfall. Companies are threatened by the increasing number with some of them failing to venture or enter into agreements based on such threats. The costs is not only translated through some of these activities directly but also implications on employment opportunities. This is further worsened by the fact that as US seeks to fight the vice, the NSA on the other hand is conducting the same activities causing massive losses on the US's economy as companies fight for to repair the damaged reputation on exposure of consumer information without their consent.

Although the proffered is one of the major threats, it is evident that United States stands to lose due to their actions on invading companies globally in the name of security. The respective undertakings that the NSA is taking are likely to cause hundreds of millions of dollars annually, especially through lack of investments and drop on sales on some of their global technology companies. The damage on reputation which is attached to the invasion of a given company based on the NSA's surveillance. Researchers

indicate that consumer's purchase products and services based on the company's reputation (Sanger & Smale, 2013). On the other hand, it seems that NSA's strategies are damaging company's reputations in United States hence scaring away investors. The stipulated analogy indicates the possibility of the United States losing on both ends that is, based on the billions of dollars on cyber espionage and also on scaring away investors.

Loss of Sensitive Information Such as Possible Stock Market Manipulation

This is one of the leading threats that companies are currently experiencing, loss of sensitive information of customers or strategies can reflect marginal losses to an organization. Loss of sensitive information of customers as experienced lately by some of the leading global corporations has caused increased concerns reflecting marginal losses to the respective companies. These organizations are not only suffering marginal losses from the consumers but also damages on reputation with the customers likely to pursue legal solutions especially when such information is used against customers with or without consent. These cases have been on rise in United States with cases of broader and regional implications rising due to cases where organizations or agencies have acquired information from other nations' organizations without consent. Competitors acquiring sensitive information of a given company also reflect marginal losses to the company.

This is based on the fact that such companies suffering such a loss are not able to create a competitive advantage within the market with their strategies being used by the competitors to gain the competitive edge. Lack of strategies or initiatives to validate, secure and policies to govern and limit such activities, have caused marginal losses

reflected into the economy. Stock market manipulations also forms one of the global implications that companies are forced to avert. Such cases are likely to have marginal losses to the global economy affecting nations worldwide. The NSA's use of information of some of these companies without their consent is likely to have massive losses as the affected organization loses sensitive information to the competitors while also damaging consumers trust and royalty. This reflects economic implications to the company involved and the entire nation in general.

Opportunity Costs, Service and Employment Disruptions and Reducing Trust for Online Activities

Loss of intellectual property or confidential information from companies or organizations is causing companies massive losses. Such losses are forcing some of the small firms out of the industry. This reflects in unemployment based on the fact that these small companies may not be able to develop new products and ideas to stay competitive within the industry. The increase in these attacks are also having marginal implications to companies that largely rely on online activities. Consumers are not confident on some of the most reliable services with companies forced to develop restrictive security measures aimed at strengthening their online services to assure consumers confidentiality. The high number of losses suffered by the consumers through online based theft by hackers, to some of the leading global organizations has largely reduced their trust for online activities as consumers divert back to the pervious forms of services.

These activities not only disrupt online services but also introduce new services with crime and drug highly increasing. Through some of the malicious cyber activities, drastic growth on drug activities has been experienced in the global market. The outcome of such an analogy is an intriguing question on whether the world can account for the drug trade's value. Based on report by the United Nation Office on Drugs and Crime, estimation was made of over $870 billion on overall cost on transnational organized crime. The estimate indicates that over $600 billion of the availed figure is generated through illegal drug trafficking. The notion translates a scenario where the similar figure can be estimated on global GDP share. The large number of these cases is mainly recorded in the United States based on the survey. These crimes are conducted within and beyond the United States borders causing a global concern on the reliability of online services and respective transactions.

The marginal implications of cyber based malicious activities on the job are diverse depicting the need for further studies. However, based on some of the estimates made by the Commerce Department, in 2011 around $1 billion in exports equaled to around 5,080 jobs, the notion depicts the high end estimate made of $100 billion in losses from cyber espionage can translate to over 508,000 lost jobs (Gjelten, 2013). The outcome reflected notion on the high number of jobs indicates a possible reduction by third of a percent based on the analogy that these workers will acquire jobs. Through the displacement that is normally made by the cyber espionage, people are not able to acquire job opportunities that can be able to pay well or better.

The outcome on a given country can be worse based on the high unemployment rate experienced. This can also reflect cases where cyber espionage is likely to lower workers from the highly paying blue collar jobs to lower paying work or even unemployment as proffered in above analysis. Although the US is enacting strategies aimed at minimizing the respective implications, the fact that NSA is indulging also in similar activities presents an intriguing parallel based on effectiveness of the means used. Although US has some of the most restrictive laws on the cyber crime issue, the notion that they allow some of their organizations to indulge in similar activities violates such analogies.

Additional Costs of Securing Networks, Insurance, and Recovery From Cyber Attacks

Based on the risks attached to these attacks, companies not only in the United States but globally are enacting strategic measures that are aimed at averting and reducing these attacks. Such measures based on different research include; insurance and developing more costly strategies to secure the networks with an aim of recovering from these cyber attacks. The additional cost of securing the networks not only cause's marginal operational costs to companies globally but also reflected to the final consumers. The notion attached to the proffered assumption is based on the fact that organizations aim at maximizing profits while minimizing on the operational costs. They are forced to reflect the respective damages to the final consumers as they increase their network security. The need to avoid losses on information leaked to the market and other

legal claims while also aiming at assuring customers on the confidentiality of their websites and online services, these organizations are forced to reflect the additional costs on to their products affecting consumers and economy in general.

The huge figures estimated to be used by companies to secure their networks and insuring them is causing economic fallout especially in countries with weak security system likely to be attacked. Some of the small companies unable to meet the costs of securing networks through insurance among other measures have been forced out of the market or industry based on theft on the intellectual property used by the major competitors. This has enormous implications to regional and global economy causing unemployment among other economic damages.

According to Tom Gjelten (2013) companies with a weak governed space are easily to be exploited by some of these attackers. This has caused a steady rise on the piracy with the different studies indicating massive losses caused by piracy. For instance, marine trade estimated over $7.8 trillion annually in 2005 (Richards, 2009). Based on the technological developments and innovations, the figure could have doubled or tripled by now. Such massive losses to some of these companies are forcing them out of the market or industry hence causing massive economic implications globally. The same notion can also be reflected on another damage termed as "pilferage", where companies are forced to embrace it as a part of cost of conducting business. Also termed as inventory shrinkage, the implications have been diverse especially in United States with the retail companies are experiencing massive losses. The conception on these losses in United States is estimated to be $70 to $280 billion with the perception attached to the pilferage theory

causing some of these companies unable to trace the loss. Therefore such implications have an invisible hand forcing them to make decisions over the acceptability of the losses based on inadequate information available (Gjelten, 2013). The same notion has been traced to spread from United States to other regions across the globe reflecting massive losses to the global economy. The need to enact measures to protect networks, with immense losses being experienced, has made some of the security organizations and insurance companies develop strategies aimed at largely creating a new venture.

Reputational Damage to the Hacked Company

This is also one of the components of cyber espionage where the company involved on these attacks not only incurs costs but also damaging reputations. This is evident as experienced by some of the global leading corporations that have been hacked. The belief that United States and other countries such as China are some of the leading nations involved in intellectual property theft have raised concerns as nations blame each other on the strategic measures enacted. Based on these contexts, the United States not only has to experience the high cost of malicious cyber activities but also repair its reputation on regional basis's such as the transatlantic regions where cyber espionage has led to enactment of regional policies aimed at setting regulations to govern these activities.

With around $100 billion cost annually, cyber espionage and other cybercrime activities are increasingly becoming a threat to the nation. The nation in return is also channeling more costs on research and development translating to $400 billion annually

with $100 in stolen IP failing to translate into the $100 million in gaining for acquires (Richards, 2009).

The proffered analyses provide a detailed approach on some of the diverse economic implications attached to cyber espionage. The specific study not only affects the United States but also other nations globally. However, United States receives excessive pressure from other regions based on the fact that it forms one of the leading contributors and apparently continues in spreading the vice. Therefore the US and other nations have to constantly review their trade secret protections through integrating efforts from the private sector and the governments towards enacting policies to address the issue.

Some of these efforts include: having a tight trade secret protection that is more advanced than in other nations in the world, with the civil and criminal previsions enacted towards addressing trade secret theft where cyber related attacks on corporate networks are attached. Under the national level, European regions insulate the United States on providing consistent and robust trade secret protections especially across its members states. Based on some of the current events and trends in United States, the European Union is evaluating options on policy formulation towards improving the regional trade protection, especially that emanating from cyber espionage. Some of these policies include: reviewing their current cyber security, incorporating efforts aimed at strengthening strategies to counter cyber attacks, and increase on secret trade approaches on regional basis (Jabeen, 2013).

Although United States is one of most affected nations, with dynamic strategies and restrictive regulations and laws governing the issue, the issue in the rest of the world is based on weak and ineffective laws or enforcement practices. This has largely undermined the efforts to address the issue. This is evident especially in the largest emerging economies such as Brazil, China, India, and Russia where the problem is acute. This has led to different suggestions towards addressing these rising global challenges through protecting and enforcing strict policies to protect trade secrets in organizations. Such suggestions include companies contributions towards providing proactive investigations on trade protection through viewing the expenditures, attached significant investments on preserving and enhancing value rather than sunk costs.

The European Union plus the respective member states are currently evaluating their protection measures based on the increasing number of trade theft. The region also known as the Transatlantic region fails to have a harmonized trade secret protection system, thus the current initiatives one needed to develop policies aimed at addressing responses at the transatlantic region. The analogy attached to the above entity is based on the fact that the US, which has been largely offering those services has been experiencing similar threats, consequently the change of perceptions by these regions on whether the United States is capable of offering effective and reliable standards.

Member states in the region have differing cyber security strategies or policies, with the survey conducted indicating similar equivalence on the trade secret protection. The level of the protection and effectiveness of the protection normally varies across different members. This respects disparities across the region capable of being protected.

The regions amid the wake of United States rise on cyber espionage is developing strategies backed up by some of the different suggestions that are aimed at improving their trade secrets from cyber espionage.

Some of these suggestions includes; providing consistency as to the different forms of information which can be protected, addressing some of the difficulties in relation to obtaining evidence of misuse and also damages, making available effective preliminary plus effective final injunctions, developing strategies to ensure that courts have the knowledge coupled with the resources of protecting secret information during proceedings, and also significance of providing for effective civil actions plus criminal remedies. The analysis provided outlines some of the effective strategies based on the suggestions made to curb cyber related crimes by governing their territories.

The changing perceptions with US in relation to the Transatlantic region based as an impact of cyber espionage therefore causing an economic fallout as the region seeks to develop their own policies is based on different facts. Value extraction from computers of some unsuspecting companies and government agencies has grown into a big business. The ability of the hackers to access information across different regions forms an intriguing entity behind changing perceptions with United States in relation to the transatlantic region. The recent cyber espionage act by the NSA in hacking on one of the most influential persons in the region (Germany) can also largely attribute to such a scenario.

Attacks against banks plus other financial institutions can likely have massive implications costing hundreds of millions of dollars every year. Developed countries are

the most affected with an estimate in billions of dollars lost on their economies deriving from cyber theft and intellectual property, plus the businesses confidential information. The fact that organizations are not aware of when or where these attacks are likely to strike continues to pose a threat to their cost of conducting business or even a major risk that the companies may be willing to undertake, this can also be based on illegal acquisitions, thus damaging the global economic competitiveness and also undermining the technological advantage. Backed up by such entities with United States being among those affected, the transatlantic region has the reason to change perceptions therefore they need to develop their own policies and standards. The difficulty on estimating the value of intellectual property is causing companies to record losses, while being unaware of the source or what has been stolen. Surveys are some of the commonly used mechanisms to estimate the costs with the failure to enact strategies at the initial stage where estimates on cyber espionage were quoted as few billion dollars to currently hundreds of billions.

Conclusion

The availed analysis defines the impact of cyber espionage changing perceptions with the United States vis-a-vis the Transatlantic with economic fallout being one of the major implications. The major way to address this issue is through developing trade policy tools and utilizing them effectively towards elevating the essence of trade secret protections, promoting more effective deterrence, and also raising global standards on cyber related crime. The NSA's strategies at the moment are having ample economic implications to global companies such as Google, Facebook Inc., and Yahoo. The United

States has the largest role to play through integrating efforts and interests of other regional players while also averting such activities conducted by the NSA.

This can be achieved through U.S. initiating and negotiating on both the transatlantic trade and investment partnership (T-TIP) and Tran's pacific partnership (TPP) with the eleven Asian Pacific nations plus China. This should provide significant opportunities towards securing advances on protecting trade secrets. The United States Government is also mandated with the role of improving the international coordination among different agencies and so strengthening the responsibility for the cyber security therefore protecting trade secrets. It is evident based on the availed analysis that cyber espionage presents a growing threat of economic espionage and in trade secret theft which provides an increasing need to integrate efforts from different companies through deterring such threats and developing robust policies to respond and cooperate at the international level.

CHAPTER 3

INTERNATIONAL LAW

Introduction

Various researchers have developed diverse platforms under the issue of international law and espionage. The analysis behind the vast research conducted in this section on international law is to provide assumptions underlying the issue under the study. The main basis in these researchers' analogies revolve around cyber espionage by examining the international law on such issues and where there maybe gray areas where the current laws have not kept up to speed with the modern technological advances. Under this approach the study is aimed at offering a detailed conceptual approach in relation to the objective of the study. The escalating incidents of cyber espionage have received a vast response of researchers offering differing positions amid aiding the occurrences (Clayton, 2011). Offering detailed analysis of these scholars and their views in reference to the issue forms the baselines under which the study is developed. The preceding offers a clear insight on international laws, through examining the history of old laws and international practices related to cyber espionage among other essential aspects underpinning the issue. Another significant aspect offered in the literature review is the essentiality of developing international laws to govern cyber espionage. This is achieved through analysis of comprehensive cyber espionage international laws and the

current laws plus the historical approach and offering a framework on the significance especially in decision making and policy formulation.

Theoretical and Conceptual Framework

Defined as the use of computer networks towards gaining illicit access to confidential information mainly held by a government or other organization, cyber espionage reflects a wide range of currently expected annual losses globally. This has reflected a growing concern over cyber espionage and the intellectual property (IP) theft, especially the trade secrets with an aim of reducing the respective implications or losses. Cyber based threat have been inexistence for a long time accelerated by the rapid technological advances that has resulted to greater connectivity, data storage, increased globalized supply chains, has increased the opportunities, potentially payoff, and also breach of corporate networks and acquiring sensitive corporate data. The United States has been at the center of global controversy after the NSA's spying was portrayed as risking billions of dollars in US technology sales while also questioning the existing international laws and policies related to cyber espionage (Clayton, 2011). The impact of cyber espionage reflects numerous negative implications.

This is a detailed analysis of the previous mentioned section under existing publication analysis. The discussion in empirical research is presented where various opinions provided by a range of researchers. This includes developing a strategic approach by examining the essential entities proffered in their research. A preview on contradictions to popular opinions and notions is offered where the review stipulate some

contradiction of opinions enacted by various researchers examining the similar aspect. A summary based on the essential aspects backed up by personal analysis is later offered examining the provided literature and the personal perception. This is to ensure provision of a rich baseline under which the objectives and the hypothesis of the study are developed.

Old International Laws and Practices

Internet security concerns are as old as the internet itself and with the attacks from state actors such as of some 3,000 Chinese hackers on Indonesian government sites or the NSA siphoning up millions of phone calls, there has been a greater call international legal reform. The international law on the use of force can be traced for the argument to the reference of Article 2 (4) of the UN Charter as the general rule. The article largely limits the use of force in exception of cases of self defense as proffered under the Article 51 (Clayton, 2011). Apart from the UN Charter, the International Court of Justice through six cases has depicted the essence of customary international law and also general principles essential to the lawful resort to use of force.

International laws on cyber espionage can be traced back years ago where some of the nations enacted regulations aimed at governing cyber espionage. The sole aim of these old laws and international practices where aimed at governing the small cases recorded then of cyber espionage. Based on the arguments presented by different researchers, it is evident that the place of espionage under international law is not easy. Some of the notions that have been embedded on these activities are based on the fact

that numerous states have been spying on each other making the entire activity seem legal. However, this contradicts with some of other researchers who argue that the act of sending spies to another territory mainly breaches the norm of territorial and also sovereign integrity, hence they should be considered as illegal pursuant to the relevant legal rules.

With a detailed analysis on the existing law and policies, it is evident that there exists no public multilateral treaties which addresses the respective acts of cyber espionage, this indicates the need for remedies to be made towards the customary rules, thus determining the position of espionage under the international law. Through the basic aspects, customary law entails the rules of which emerge on the past practice among different nation states that governs the future relations between them. The State of the International Court of Justice offers a definition of the customary law as basically evidence of a general practice which is accepted as law (Duncan, 2011).

The application of international rules is normally based on the Lotus principle, which indicates that a sovereign state may not be able to undertake any action they wish as long as the action being taken is not explicitly prohibited. The analogy attached to this notion questions whether the availed analysis is an explicit prohibition on acts of cyber espionage. Although nations have been constantly spying on each other, there exists no evidence towards supporting proposition that state actors view cyber espionage basically as something which is legal under customary international law. In the indicated analysis, old assumptions and a lack of effective laws to govern the respective activities on cyber espionage, it may not offend the territorial integrity of the target such as a human spying

would. This signifies the fact that some of the intrusions are likely to offend the principle of interference under the international law. This corresponds with the fact that cyber intrusions normally offend the principle of non interference, which is correctly considered to be illegal pursuit of the respective customary rules.

The availed analysis also depicts the fact that the influence on the behavior of the respective state and non-state actors in reference to the cyber espionage are highly complicated, more so than a simple determination of legality. The correspondence attached to the given insight based on the arguments generated indicates that cyber espionage is illegal, although the vague notion of the illegality pursuant to an even vaguer general rule of customary law, which acts as an extremely poor restraint on the state behavior. The poor policies and standards combined with lack of constraints has largely increased massive campaigns by different states which have sought new international restrictions on political, economical and also military cyber espionage activities. Although the US seems poised on building a bifurcated legal system through separating the economical espionage that is aimed at private sector interests from other more traditional forms, it is evident that such efforts have not yielded much benefits towards restricting or limiting cyber espionage (Duncan, 2011). The in depth study offers a detailed insight on the respective old international rules and practices that failed to have effective implications. This has largely affected the developing of international laws and standards aimed at governing cyber espionage activities. The outcome has also been a dramatic increase on cyber espionage activities with no international legal laws to govern or limit these activities.

The NSA's Cyber Espionage Offenses, Repercussions and the Call for Legal Change

The United States has been in the center of a global controversy after its NSA department had been found spying on multiple nations, including allies. Such espionage activities had repercussions that have been portrayed as risking billions in US technology sales while also creating legal implications limiting international law. The impact of cyber espionage reflects numerous negative implications ranging from economic downfalls to a blow on international cohesion. The analysis indicates the need for legal change on the NSA's cyber espionage activities by developing effective international laws.

The decision by a congressional committee on blacklisting the Huawei Technologies Co'.s products from the United States telecommunications market, based on allegations on enabling China to spy on the United States, presents a threat on economical developments (Prodhan, 2013). The same decision is being projected to also likely affect Silicon Valley. This is based on the report by the National Security Agency persuading some of United States based technology companies to develop what researcher's terms as backdoors on security through security products, devices, and networks. Therefore allowing easier access and monitoring as the same which had been described by the House Intelligence Committee as threat posed by China through Huawei.

The implications on these cases of the China based Huawei is estimated to have business and economic effects as companies in the US failed to use its equipment.

Researchers estimate reduction on US technology sales in overseas by over $180 billion by 2016. Despite such losses and implications emerging from the NSA's actions, it comes to a be hindrance to the legal aspects based on the efforts by the international community to set laws and policies aimed at governing cyber espionage activities. A lack of consistency on international law is one of reasons that can be attributed to the increasing NSA espionage activities. In May 2011, President Obama changed the way the US would play a role in US cyber security planning, indicating that it would be international law as interpreted by those who normally advocate on a broad right of the US to resort to force.

The intriguing correlation that can be traced on such words seems to largely differ with the allegations offered by the NSA's espionage activities on other states. Although the US seems to be at the frontline on advocating for minimizing the use of cyber espionage activities, the NSA seems to embrace such activates and expand upon them. With recent allegations that the NSA had been spying on European Nations such as Germany, France and Spain, eyebrows have been raised on the validity of the US' true efforts and their technological capabilities.

It is evident that the current allegations directed to the NSA and the United States government is having massive economic and legal implications. This is also reflected on the fact that implications are also beyond financial or reputation but also across borders, this is evident based on the allegations published by the German Magazine Der Spiegel (Poitras, L. 2013) claiming that NSA had cracked encryption codes hence listening on to 1.4 billion smart phones globally including that of Apple Inc's iPhone.

The chain of allegations charged against the NSA for digitally invading some of these companies and using their information against their consent, presents an intriguing analogy on the effectiveness of dealing with international law while ensuring trade secrets laws and regulations are safeguarded. Companies and organizations such as Google, Yahoo, and Facebook Inc. have been forced to petition the United States' Foreign Intelligence Surveillance Court, that is mandated with making rulings on warrants for the domestic data, towards offering them permission to publish these types of requests that they receive from the NSA (Prodhan, 2013).

Actions on international law relating to cyber espionage have largely been dominated by disagreements on whether peacetime espionage is permissible under the international law. One of the most interesting analogies that can be traced on the international law is the notion that it was not established to address the finer aspects of the given questions. This is based on the fact that it was enacted during the heights of the Cold War and also used into 21st Century. The pursuit for the international law basically can be traced back on the 17th century as availed under the writings of Grotius. He was one of the major figures in the development and the usage of the current or the modern international law.

During that period, espionage was mainly conducted during wartime. Consequently receiving attention in international law, especially law governing armed conflicts where peacetime espionage had not been part of the aspects attached to the respective concept. Espionage according to Prodhan (2013), is not prohibited by the international law as a fundamentally wrongful activity based on the notion that it fails to

violate the principle of *jus cogens.* The concept under *jus cogens* is normally defined by the Vienna Convention of the Law of Treaties as the norm accepted and recognized by the international community of states. The fact is the international law fails to have a more effective and systematic approach. Which provides the NSA with a situation where it takes advantage of and indulges into cyber espionage activities such as, spying on other nations military, political and economic areas under the notion of security.

The legal implications and offenses by the NSA extends to companies such as Cisco. On the other hand, Cisco has indicated that they don't customize equipment specifically for enabling NSA surveillance. The allegations that the NSA had used the company's devices and gadgets to spy on other nations, not only indicates some legal implications but also marginal economic consequences for Cisco which may become significant. According to the report by some of the senior managers in the organization, they argue that their product development practices and policies do not advocate for international behavior or product features that are designed in allowing unauthorized devices or networks to access or expose sensitive device information.

The company denied the claims that they were aware of the NSA having an encryption program. The undertakings by the NSA on cyber espionage activities cripple the efforts to enact effective international law where cyber espionage can be viewed as wrongful deeds that extend beyond international protocols. The fact that the NSA spies on some of the information generated from telecommunication companies through listening in on calls and also tracing other personal information without the consent of the

respective individual or the company itself offers a disturbing system likened to a secret police.

These undertakings on cyber espionage by the United States is likely to have massive economical and legal implications. Researchers indicate that some of these undertakings being enacted by the NSA are likely to kill the United States technology industry and their respective efforts aimed at creating a stable cyber security globally. The NSA's offenses are causing massive losses to the US especially on companies which are involved in such activities with or without their consent. The US technology industry largely depends highly on overseas markets, with some of the leading companies acquiring substantial shares of their revenues from the overseas markets (Holmes, 2013).

For instance Cisco System Inc. (CSCO), which is one of the leading networking equipment makers, recorded around 42 percent of its $46.1 billion in fiscal 2012 revenue outside the US. Symantec Corp. (SYMC) is also one of the biggest makers of computer based security software located in Mountain View, California that reported 46 percent of its fiscal 2013 revenue also outside US markets. Intel Corp. (INTC) reported 84 percent based on its $53.3 billion in fiscal 2012 also beyond US borders based on data collected by Bloomberg, Intel Corp. forms one of the largest semiconductor manufacturers in the world (Holmes, 2013). The NSA's offenses to indulge into cyber espionage offer an intriguing insight on the economical implications and the legal based aspects while also deterring efforts to develop an international law that governs such activities. This depicts the need for integration by other stakeholders where policies on regional and international

espionage activities should be enacted to offer a clear international law that limits the use of cyber espionage activities by security bodies such as the NSA.

According to Holmes, (2013) these threats attached to cyber espionage among forms of cyber crime activities, strike directly at the core value of different corporations reflecting a central vulnerability likely to have substantial losses to businesses. The same vulnerability can be traced on the governments of the involved countries. Currently, the United States and China among other nations have been in constant disagreement over each of the other nation's cyber espionage activities where they have spied on one another. Recently the US produced a list of Chinese nationals and their arrest notices for being involved in cyber activities which targeted the US security system. The implications are a setback on regional cohesion as the same allegations have been made against the United States by European Union nations such as Germany, for recording calls on some of the highest political figures in the country.

The research on business implications also argues that trade secrets normally comprises an average of two thirds of the value of a businesses' information portfolio, which researcher indicates that the percentage normally rises to 70 or 80 percent for the knowledge intensive industries, such as the information service, manufacturing, scientific, technical services, and the professional services. The information and analysis above fails to address cases where some of the trade secrets made public becomes a loss to the company with their value not recoverable. Especially when acquired by the competitors. The fact that the NSA and the United States government is using such information with or without the firms consent presents massive economical implications

on firms and the United States in general. Such activities are causing regional tensions, therefore blocking efforts to enact an effective international law aspect thus governing such activities.

The cyber espionage related intellectual property total loss aggregate amount has been staggering annually. This is based on different factors within the industry with nations pointing fingers on some of the major players towards enabling the accelerating accessibility of information and the usage. This has created a vulnerable environment between firms and nations across the globe which is also transpiring legal implications on the nations involved. According to the United States Department of Defense, every year, a large amount of intellectual property, larger compared to that retained in the Library of Congress is normally stolen from various networks that are maintained by United States; businesses, universalities plus different governments departments and agencies.

The same arguments can be reflected by the a 2012 speech by General Keith Alexander National Security Agency and U.S Command, who indicated that IP or intellectual property theft due to cyber espionage declaring it the "Greatest transfer of wealth in history" (Rogin, 2012), he also indicated that United States based companies annually lose over $250 billion due to Intellectual Property theft. The problem is not mainly limited to cyber espionage as trade secret theft continues to grow in different forms with the current technological development largely facilitating such activities, the United States records over $300 billion in losses on such activities annually.

Historical trend on the growth of these cyber related theft and crimes are evident, as previously discussed, based on the fact that in the United States the federal cases

related to the trade secret theft were recorded to have doubled between 1988 and 1995, the same notion was also recorded between 1955 and 2004, with projections made of doubling again by 2017. Although the conferred analysis indicates the losses caused on firms and the global economy due to accessibility of the information by these attackers, the fact that the NSA is also accessing such information or instructing companies to develop products to facilitate surveillance without consumers consent presents an interesting dilemma (William, 2011).

Consumers are shunning away from organizations that have been involved in such cases causing massive losses. The same implications are reflected on a regional base where countries and organizations such as European Union and its members have begun diverting their reliance on US technology assistance. This is likely to have massive implications on the nation’s economy through not only scaring away consumers on some of the suspected products but also in investors across these regions. The US addresses cyber espionage caused by privatized attackers on companies and government agencies while on the other hand, they seem to exercise the same activities.

The research indicates how the NSAs' offenses are obstructing efforts to develop international law. The implications of a failure to enact strategic policies to limit such activities may have not only effect legal or political issues among nations but also economic implications. There is a need of developing strategic policies and developing legal policies where international law has a system of governing and limiting the NSA and other organizations from cyber espionage activities. Legal changes governing and prohibiting cyber espionage are required into the current legal aspect. Such changes

should be incorporated into international law for the profound reason of limiting cyber espionage in the global cyberspace.

Laws Being Enacted

The increasing cases of cyber espionage has attracted interventions by the United Nations with the need to develop solutions aimed at governing such activities, being one of the major issues to be addressed. There have been efforts aimed at changing and implementing new policies and standards that would limit cyber espionage by nations against one another and even security bodies such as the NSA. The analogy attached to this aspect indicates that the respective nations are offering legal drafts or laws which are aimed at changing the current international law on cyber espionage. The US's charm offensive within the United Nation provides an interesting message as the United States terms their respective cyber espionage activities as security based measures (Vida, 2008).

However, the fact that United States has been accused of spying on European and South American counties such as Brazil and Germany, questions the United States policies and regional unity goals on integration between these countries. It is evident that there are marginal implications on economic, technological and political based issues that emerge from cyber espionage based activities. These activities are threatening regional ties which is likely to have negative implications on the regional and the global environment. The notion attached to the proffered entity indicates the need to develop policies and change the current legal measures on cyber espionage towards meeting

international standards. This is essential towards ensuring that there exists an international law that prohibits cyber espionage activities.

Germany with the support of Brazil are two nations that have brought a draft to the United Nations over the need to end global digital espionage. A draft presented in November 2013 had called for the need to extend the internet rights to privacy which should be enshrined under the International Convention and Political Rights. The efforts by the two nations were spearheaded due to the United States' actions against some of their political figures. Although the United States denied such claims, the actions by the two nations presents a clear insight on the significant implications on the accusations directed towards United States. The draft to the General Assembly affirmed that similar rights that people have offline should be also protected online especially the right to privacy. The draft resolutions were aimed at altering the current policies and standards that tend to offer loopholes where nations can attack and spy on another without international law that governs or limits the effectiveness of the system. The presumption embedded under the draft stipulates how the United States and other nations such as China needs to be restricted from spying or attacking other nations through developing international law to govern such actions (William, 2011).

The draft was aimed at confirming the right to privacy while also calling upon all nations to protect the right of privacy. It also proffered on the essence of enacting policies and strategic measures that are aimed at ending the violation of such rights while also creating and implementing the legislative measures that are related to spying, interception on such actions, extraterritorial surveillance of communications and also the collection of

personal data of a given massive surveillance, and also the interception and the data collection. The correspondence on the need to make the changes and implement the respective required measures was altered by the Brazilian and German Diplomat while presenting the draft to the United Nations, with the aim for pushing against cyber espionage. This also indicates the fact that there is a need for the respective nations to contribute to the development of the document, plus also demonstrating that they are ready to take care of what had been perceived as one of the acute problems in international humanitarian law (Vida, 2008).

Brazil and Germany presented the draft with an aim of introducing changes to the current international laws, which fails to fill some loopholes that nations exploit with their cyber espionage programs. The document provided a clear cut and dry stance on tactics, and or states that illegally use surveillance upon others, which are in violation of the rights of privacy and the freedom of expression, while also undermining the foundations of democratic society. The draft offered to the United Nations, urges the global body to offer protection on the right to privacy under the framework that is; domestic context and the extraterritorial also including massive surveillance of communications and the respective interception and the collection of the personal data. The heightened accusations by the two nations came amid cases that the United States had recorded the German Prime Minister's (Merkel) phone call and also monitored the Brazilian (Rousseff) and Mexican (Nieto) Presidents text messages and phones call as well (Boadle, 2013).

The purpose of this analysis offers some of the currently enacted or recommended efforts that are aimed at setting new international laws and policies to restrict nations from spying from each other with legal implications imposed on those that indulge in such activities. Although these laws may be implemented, their effectiveness towards curbing cyber espionage issue has not yet been identified. The increasing technological developments and advance of more complex devices may undermine such efforts. The implementation of such policies may not also fall under some regional aspects as some of the nations are not under the United Nations umbrella. Such nations may not validate or see the essence of following as the enacted laws and policies consequently violating the set parameters.

However, the implementation of the recommended laws, policies and governing regulations may govern some of the nations from executing such activities. The analogy attached to the concept is that states may be required to follow a set international laws under the draft recommendations to avoid international sanctions. One of the limiting entities under this concept is that some of these activities are not necessarily executed by the government. Some of these spies can be illegal firms or individuals with the capability of attacking and conducting cyber espionage activities against another state. The international law and the recommended policies and changes largely advocate for the state to state or regional based legal issues, however the fact that such laws and policies are not embracing the private based illegal cyber attacks, offers an bewildering concept. The effectiveness of the recommended policies and standards is vital towards governing

cyber espionage activities although they need to consider some of the aspects on private and government based entities.

Conclusion

International law on espionage activities based on the provided analysis, has illustrated how the international community and the UN have failed to effectively govern states from indulging into such activities. There are substantial implications attached to the failure to enact strategic legal measures and policies to limit such espionage activities. The legal rules and the conducts have failed to limit cyber espionage activities thus far. The regional implications transpired by the NSA's actions to spy on other nations such as Germany and Brazil is reflecting moderately on the US economic, legal and political based entity. The current draft presented by Germany and Brazil to United Nations with some of the recommendation on the necessary changes that can be made on the current international law are some of the vital undertakings that every nation should embrace. How far this push against the US goes is still to be seen with the fluid situation.

The United States is also largely pushing for the creation of a normative and a legal framework aimed at prohibiting the acts of economic cyber espionage. This is based on the fact that the United States stands to have substantial losses compared to the gains. The United States generates the highest amount of intellectual property with the firms largely depending on sensitive and proprietary information regarding their respective business activities and practices. However, the United States may not benefit through cyber espionage, the damages may be extensive on their economic and legal based issues.

Other nations may help develop an enduring reputation for the United States. The nation should be in the frontline not only fighting for the implementation of legal policies governing economic espionage, but also developing international law to govern and limit cyber espionage activities. The essence of enacting some of the recommended legal strategies by Germany (and Brazil) indicates the basis of ensuring that international law is amended to integrate the right for privacy with cyber espionage activities deemed as a violation of privacy.

The value of lost information through cyber espionage is certainly great. This indicates the need to enact strategies that are aimed at embracing "Moratoriums" based on cyber espionage. The efforts on some of these strategic and legal policies should be focused on as countermeasures, capabilities and also some open lines of communication which are aimed at thwarting potential conflicts due to misunderstandings between states. In addition to acting as a conflict diffusing mechanism on the international spectrum with regional and global affects. The essence of an international law that governs the respective undertakings and activities of cyber espionage, while also ensuring that states maintain their privacy, is required. This can largely aid in developing policies as discussed in the study. Some of the gaps on the analysis conducted falls under the concept of how to enact and the respective implications of international law hence the need to carry out the study.

CHAPTER 4

SYNTHESIS

I have learned that this year has possibly been a turning point in terms of transatlantic cooperation's. This is on the backdrop of the culmination of NATO combat operations in Afghanistan with the optimization of the increased overall trend in relation to the potential implications that are profound in terms of crisis management. This as well as the "Out of area" operations that no longer suffice as a form of glue and justification in terms of security and defense in regard to the relations among transatlantic member states. In the same instance outlines exist of new relations that remain as emerging which leads me to single out the three "Drivers" that are the most relevant in the shaping the context where cooperation rests. These include constraints to finance and resources, the transformation to an increased internal perspective of the European Union as well as capital of NATO with the final aspect being the shift of power relations on the scale of international systems. I have also learned that the revelations of Edward Snowden in terms of the scope of surveillance as conducted by the United States and its intelligence agencies have been under the subjection of increased debate in Europe more so in Germany.

The United States and the United Kingdom have had a long running and sustained agreement in a multilateral format based on the cooperation in regards to signal

intelligence. This partnership is between the nations of the United States, the United Kingdom, Canada, Australia as well as New Zealand with the joint intelligence operations known as Five Eyes. In the course of 2013 leaks by the United State's National Security Agency in the scandal of internet spying led the surveillance entities of the Five Eyes to face accusations of spying intentionally on the citizens of each other. The allegation was that laws were circumvented with the aim of prevention of these agencies from undertaking espionage operations on their own citizens. The leaks of the U.S National Security Agency were not entirely a new matter but instead were a sort of confirmation of disclosures that had been made earlier regarding the UK-USA espionage alliance.

A Test of Partnership

This is because it was treated with surprise in several circles as the nations are the closest political ally of the United States and yet their private communication was intercepted on an extensive scale. This went as far as wire tapping of officials of high rank within the European Union and its member states as revealed in the later National Security Leaks of 2013. More so the United States government continually applied espionage mechanisms on the most crucial internet platforms of daily utilization by Europeans which include Google, Yahoo and Amazon among others. Acquisition of information pertaining to European citizens using means and methodologies were fundamentally opposed in terms of legal sensibilities according to Europe. These were called for since it was the right of European citizens and governments to fundamentally

call for self determination of information. Such practices have created damage to the transatlantic partnership with Europe and the United States as well the possibility of outcomes as a breach of trust that will prove to be irreparable (Burmester, et al. 2012).

From this I have understood that certain international intelligence policy observers present the argument of intelligence sharing partnerships with varied interests and beliefs in structure of intelligence gathering. This is possibly due to the lack of an adequate balance amidst cyber security and protection of data. Therefore, reconciliation as a product of the geostrategic positions are often diverse and indifferent. Due to the engagement of the United States in an increasing global scope, I have come to understand that threats to national security will likely be more serious compared to those that Europe faces. It is for this reason that Europe and America are not likely to seek a ground that is common in regards to policy of cyber security as well as protection of data in the near future (Nye, 2011). Indeed, these forms of cooperation are enshrined in the framework of multi international stakeholder-ship on internet based governance have been taken for granted in the past, with an increasing possibility of controversy in the future. Even with the present chilly relations being under an cyber espionage test, the coorporation of transatlantic partnership continues to be foundational since it provides normative and institutional benefits.

All concerned parties however have come to an agreement of the primary aspects in the regulation of the internet which is based on the conviction of access that is universal in regards to internet. This is extraordinary pertinent not only in decision making on the democratic basis as well as in free markets but also for the future

liberalization of order that is democratic. Therefore, all sides are in unity as well as the search for means that are effective in the limitation of software that is malicious in fighting crime as well as securing infrastructure that is critical. The controversy that surrounds the espionage activities of the National Security Agency have brought exposure of the variations between the United States as well as member countries of the European Union. It is on the basis of the consideration of the means of intelligence that are illegitimate and their common application that raises the greatest concern. This revelation has also been made as directed to the approaches in managing the dissonance among transatlantic partners that is normative. Nonetheless, the overall aspect of transatlantic intelligence partnership has been misunderstood since the threat is existential (Nye, 2011).

Rather, the transatlantic variations need to be resolved in a speedy manner using political dialogue with major areas of challenge being diminished within mutually beneficial outcomes. In the global approach, the current mode of internet regulations are in a lopsided manner which are in favor of the United States, although it is not sufficient in terms of integration with powers that are emerging such as Brazil, China and India. Let alone the existing power of the E.U. The conceptual framework of "multi-stakeholder governance" can be defined rhetorically in terms democratic although governance of the internet (Burmester, et al. 2012).

Actors that are financially weaker yield precious, although minimal, influence and yet it is central to institutions for instance the Internet Corporation for Assigned Names and Numbers (ICANN) or in another case the Internet Governance Forum (IGF). It has

been observed that the United States and Europe have been vocal of their unison in the governance that exists as a long term model of multi-stakeholder governance in regards to internet governance. Present disclosures over the surveillance practices that have been conducted by the United States on the other hand have caused increased questioning among Europeans in concern of the status quo as well as the realignment of the balance of multinational state power such as Brazil, that are being undertaken. On the other hand in the transatlantic approach the United States and Europe have shown a divergence that is sharp in regard to their views on the most crucial objectives in terms of transatlantic cooperation among national governments (Franklin & Larry, 2008).

This was in the arena of cyber security policy more so in regard to the appropriation of the balance in terms of security as well as freedom. The cyber security policy of the United States is driven with an increase of the military logic as a deterrence that entails the sustained and strengthened offensive in terms of capacity. On the other hand Europeans deal with aspects of security as a matter of the police with their main objective being the strengthening of their systematic resilience as well as resistance to being attacked as well as fraud. In accordance, the United States and European intelligence entities are varied in the fields of responsibility as well as authority.

This is aimed at the prevention of such variations in terms of the extensive conflict from both sides which presents a call for engagement by all parties in a more open manner. Therefore, success is dependent upon the United States and Europe in terms of their recognition of both sides, limitation of domestic policies as well as the range of compromise that is feasible. With the continued search by the United States of

sustaining a position of dominance as a global power I have gained the understanding that its cyber security policy will remain to be motivated by matters of national security (Burmester, et al. 2012).

Therefore, the drive will also be military logic as deterrence whereas for the European Union questions concerning data protection will persist to be of main significance along as the approach to cyberspace is driven by the police with emphasis on improvement of the capacities that are defensive. It is only after these limitations are held in respect that all countries will be engaged in cooperation that is mutual in terms of policy of cyber security as well as governance of the internet.

It is only after such limitations are held in respect that mutual cooperation of cyber security activities in terms of policy as well as governance of the internet can seek certain ground that is middle and also pays off for all parties (Nye, 2011). Furthermore, on the transnational approach I observed that the partnership of transatlantic stakeholders with the involvement of varied perception of a well structured relationship of citizen and state, needs to be upheld. Unfortunately, such requirements necessitate attention that is urgent in timing when mutual trust among states as well as its citizens face erosion. Disclosures have allowed for sensitization of citizens to the dangers that are inherent in terms of the digital revolution.

The possibility remains of the trust by the public in terms of safety of internet based communication that has been shaken deeply with certain circles making demands for the renationalization of information as well as communication technology based infrastructure. This is being in a run up to negotiations regarding the Transatlantic Trade

and Investment Partnership for instance the demands for formulation of supranational legal resources as well as independent bodies that provide mediation with voices already gaining pace. Furthermore, I have come to learn that in years to come the European Union as well as the United States need to get used to countries that are emerging such as the Brazil, India and China (Burmester, et al. 2012). This as their demand increases in frequency with the utilization of agreements that are multilateral in regards to internet governance within the procedures of multi-stakeholders. The US and EU transatlantic regions will have to learn how to evolve as others nations rise in influence.

Initiative and Transatlantic Principles

The transatlantic cyber security partnership with the European Union and the United States has undergone development as well as strengthening over several years. Associated policies in both regions share commonality that is normative in accordance with the foundation and principles of regulation augmented by the characterization of domestically political debates that are similar with regard to increased appropriation in regulation of the internet structure (Franklin & Larry, 2008). The internet as a cyberspace platform is an international and public space as well as an economic instrument which is positive as it spans the entire globe. Aspirations of regulation of cyber partnerships are not restricted to the transatlantic area but instead concern the entire spectrum of information technology systems that are structured according to data networks on a scale that is global.

The United States as well as member states in the European Union share a similarity which is being based according to service economies where an extensive proportion of economic activity is under the transaction over the internet. Their essential economic infrastructures with the inclusion of energy as well as sectors of transportation are dependent on the stability of channels of communication. This is improved by usage of the internet in regions that are economic, recent increased levels for the year which has exceeded the levels in numerous other countries. Nearly seventy five percent of European households boast of internet connectivity, while Southern and Northern American households have nearly sixty one percent being in connection.

With such similarities there is no surprise that the European Union is applying to the International Strategy of Cyberspace formulated in 2011, to provide guidelines for the development in the personal unification of cyber space policy (Nye, 2011). In combination with international partnerships as well as organizations the private as well as civil societies as well as the European Union are demanding the formulation of policies that provide assistance to the guarantee towards the preservation of open, free in addition to security of cyberspace in service to bridging the digital divide.

Multi-stakeholder Model

With certainty the main feature in the United States as well as the European Union in terms of internet governance insight is maintaining a collectively positive environment. This has natured dependency of universal free online accessibility. This has

been guided by the principle that is normative for citizens of transatlantic partners being able to freely use the internet to the full possible extent with no fear of being spied upon.

More so the internet needs to be under subjection of national laws which are applied to hardware and software platforms in accordance with information and communication technology standards. I have learned as such the sharing of principles that are normative of the transatlantic cyber partnership. This is sought in the expression that is shared in terms of the perception of the requirement of the internet and the approach that can be regulated. In part of the United Nations World Summit on Information Society follows the dispute with China and the United States from 2002 to 2005 arising from concerns of management of the internet (Burmester, et al. 2012).

The argument rests on whether private entities should be charged with this responsibility or public authorities with the preceding response in question, being the Working Group on Internet Governance. This was developed by then Secretary General Kofi Anan who formulated the multi-stakeholder model that was in support of over 190 nations as an acknowledgement of the internet not having a central authority in governance. It was noted that the internet was a rise of the outcome of interaction of all participants as well as stakeholders who are concerned with the inclusion of government as well as business.

Domestic Debating

The research and analysis of this study has provided an understanding of transatlantic partnership, intelligence and the ramifications of the fallout among member states in light of the National Security leaks of 2013. The international debates over the conflict concerning internet policy in the European Union as well as the United States are all derived from their domestic political bases. When their citizens became angry the politicians acted reflexive and with haste. The business sector also functioned in a similar nature. Once their customers exerted grave vocal concerns which was followed by a loss of consumption, such cooperation responded to the respective governments.

All of this is in light of the discussion of unlimited access to digitally based information and infrastructure in the aspects of an intelligence community's geographical reach, as well as speed in terms of data collection and mining. This creates hope that the international community and global citizens continue to have a voice, which include considerable measures in addressing matters of restriction, accessibility as well as legitimacy. Though, the international community must have access to information in regards to what the secret intelligence institutions are conducting and where they are violating the essence of their privacy. In addition, to the other states who are not within the clandestine collective organizations who are blanketing the globe with micro and macro operations, the US must take action. For the US to resolve the conflict with its Transatlantic allies it must be willing to include them within their intelligence apparatuses and in doing so, this will provide stronger safeguard measures to help prevent institutions from overreaching, which strengthens the diplomatic cords between them and provides stronger economic cohesion through information transparency. Continuing to

building broader and deeper diplomatic ties and working together to create a universal legal framework on cyber espionage activates will only make the digital and physical security within the states stronger and as well to increasing the protection of their citizens.

CONCLUSION

Liberty and Equality in Transatlantic Cyber Security Norms

In conclusion, as suggested by research in the previous chapters there has been a significant shift in terms of cyber security development with progress being directed to certain major areas. This being amplified by equally vital setbacks coupled with a development of solid implications to the foreign policy of the United States. This is in addition, due to the occurrence of the transatlantic cyber espionage operations on the backdrop of very important shifts in the international strategic environment. As such in the forward direction it is essential for the United States to undertake a reassessment of its present strategies regarding cyberspace with the placement of efforts as well as resources where they are needed the most. Exploiting the realm of cyber space by utilizing it as a developmental theater for offensive capabilities that are unprecedented has led to a transformation of the attributes of warfare. Offensive cyber abilities have risen in addition to the incorporation with the military equation of prominent and less prominent global powers as well as by non state actors.

Therefore, even in the face of these vital developments, serious obstacles remain with the inclusion of attaining the agreement of how to handle international cyber security situations. This on the backdrop of the United Nations Charter, international laws and as well as armed conflict laws in application with this new age. It should be noted

that Europe and the United States both share the same interest in moving collectively towards the promotion of stability in international trade on the basis of the rule of law, with accountability and as well as measures that are impartial. In addition to such standards, there is also an overarching regard to democratic governance and the rights of individuals that continue to face varied interests which endure to pose as obstacles in the complex international political arena.

National Security Agency Leaks and the Derailment of Transatlantic Cooperation

Cyber security is one of the most salient aspects when it comes to such challenges with cyberspace's primary concern of information protection, in terms of intellectual property as well as personalized information. This digital technology protection is aimed at the reduction of the associated dangers with the disruption to vital infrastructures and the environment of cyber security itself. These are dependent on the damage to innovation or human rights, in which several nations share an understanding of the risks faced in cyberspace that are normally associated with political differences and often creates challenges to collective action.

Cyber security demands global cooperation to formulate a cyber environment of stability and increased security. This is based on the premise of the United States and Europe working collectively towards the shaping of the foundation of cooperation as reinforcement to security and democratic values. Prior to the revelations of the National Security Agency the United States and Europe worked in a close relation towards the definition of responsibility in terms of state behavior in the realm of cyberspace. Though,

the discoveries concerning the activities of the National Security Agency had created an environment of turmoil. This disruption impacted the pace of cooperation as well as the scope of the cyber security between the two entities.

The leaks of former NSA employee Edward Snowden brought to the forefront the global dependency on the international networks, the inherent vulnerabilities' within cyber space and the inability of any state to disconnect. Cyber security needs agreement among nations, although the foundation for such agreement needs to be based on trust in order to abstain damage. The reaction these leaks presented were varied among nations, with the German reaction being pronounced with demands that may require possible increased attention to the protection for the data of its citizens in the near future and in any of its cooperative activities in cyber security. The French response was mixed but then it dwindled. Overall it was acknowledged their agencies spy on other nations as well. Varied reassurances in the trust as well as political and commercial interest present a complication in the rebuilding of confidence in the transatlantic partnership.

These disputes concerning strategy remain unknown in the face of European domestic policies as well as in the United States' national security policy. Though as long as there is a lack of clarity in regards to strategies between the US and the Transatlantic states, there will remain a lack of trust with a tendency of clashing. When compared to the past, democratic norms are currently in a state of vulnerability. Furthermore the strengthening of efforts towards authoritarian regimes has created an unintentional restriction of freedom in cyberspace. But when such disputes in the past have had a

possibility of weakening the international defense of human rights, more often than not democracies rose to meet the challenges.

Cyber Security International Politics

Without the cyber security leaks there would have not been an amplified motivation for the reassessment of cyber security itself, despite the fact that the larger traditions that shaped and held the perceptions of cyberspace are no longer an indication of the political reality. The perspective held by the pioneers of the internet platform, more so the United States' technical community, was hindered due to the lack of cohesion in states where civil societies held the assumption of varied traditional functions of governance. In a retrospective, such assumptions are invalid since governments had experienced increased attacks of cyber espionage, which enhanced the correlation of unity among states to the point of possibly adjusting the internet platform, political security and economic impacts. Though countries that remain politically dominant in the international area are viewed as being steady with increased expansion in terms of sovereignty in controlling cyberspace as governments make attempts at managing risks as well as gaining advantages from digital networks.

The legitimacy of the European countries complaints regarding to espionage still remains, but if concerns are carried to far the actual risks that remains to these nations as well as the United States, will continue to grow and compound. The main aspect in the transatlantic security lies on the construction of international systems that operate on the basis of the rule of law with peaceful dispute resolution as well as the respect of human

rights. Both Europe and the United States had grown in wisdom through the painful lessons following the era of the Cold War. Therefore in regards to the leaks, strong and sincere efforts have been made towards the remediation of political impacts in a wider structure of the norms in terms of governance and security of cyberspace.

Transparency of internet governance, the clarity in expectations regarding behavior and improved cyber security remain as key components of transatlantic cooperation in the aftermath of the NSA leaks. To avoid escalating the conflict between the US and its transatlantic allies, there are certain measures that will need to be worked trough mutually. All partners in transatlantic cooperation will need to take action in order to attain transparency in cyber security. There is a necessity for the United States to bring its practices of espionage into a level of accordance to a standard of espionage as established mutually by the parties with common ground found on all sides. This will have to be carefully married with individual states rights to national security and national protection. In addition to the demonstration of commitment to political restraint and as well as proportionate to the privacy in accordance to European expectations. This requires measures to be undertaken by the United States in reassuring its European partners in addressing its concerns towards the European public. This is augmented by the establishment of new approaches to working with organizations such as the European Commission in enforcement of legal competencies. As a result this will require member states to formulate a communal definition of the scope of actions that can be undertaken as well as the best approach to the cooperation in advancement of transatlantic security as well as international human rights.

After analyzing the cyber espionage conflict within the US and its Transatlantic partners, it is clear that the measures described above can move the situation from political, economic and legal quarrels, and on to a path of peace building. Though any future breaches of sovereignty from cyber espionage more likely than not would pose setbacks to the allies in rebuilding their natural level of peace. The US and its Transatlantic allies discussions must be on a level of transparency, minding state security. There must be common ground and mutual standards which are off limits and agree upon. The emphases is on the sincerity of the governments and their leaders.

REFERENCES

Aftergood, S. (2000). "Secrecy Is Back in Fashion," *Bulletin of the Atomic Scientists*, 56(6), 24-14

Aldrich, G. (2000) "The FBI: Managing Disaster?" *Shield*, Spring 2002.

Arensman, R. (2000). "Keeping Secrets," *Electronic Business*, May, 2000.

Arsanjani, M. H., Cogan, J. K., Robert S., Sloane, R. D., & Wiessner, S. (2011) *Looking to the Future: Essays on International Law in Honor of W. Michael Reisman*. Ed. Mahnoush Arsanjani. Leiden, The Netherlands. Martinus Nijhoff Publishers.

Ball, James et al. (2013, Dec. 13). "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications." *The Guardian*. Retrieved from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Boadle, Anthony. (2013, Sep. 2) "U.S. Spied on Presidents of Brazil, Mexico-Report." *Reuters.* Retrieved from http://in.reuters.com/article/2013/09/02/usa-security-brazil-mexico-surveillance-idINDEE98108U20130902

Bamford, J. (2001) *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century.* New York, NY Doubleday.

Barboza, D. & Drew, K. (2011, Aug. 3) *Security Firm Sees Global Cyberspying*, N.Y. TIMES. Retrieved from http://www.nytimes.com/2011/08/04/technology/security-firm-identifies-global-cyber-spying.html?pagewanted=all

Barton G (2002, June 27) , *Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say*, Washington Post. Retrieved from http://ellen-bomer.com/Osama/Cyber-Attacks.html

Berkowitz, B. D. & Goodman, A. E. (2000) *Best Truth: Intelligence in the Information Age.* New Haven, CT. Yale University Press.

Boadle, A. (2013, Dec 1)). "Brazil, Mexico Ask U.S. to Explain If NSA Spied on Presidents." *Reuters*. Retrieved from http://www.reuters.com/article/2013/09/02/us-usa-security-brazil-mexico-idUSBRE9810B620130902

Burmester, M. Magkos, E. Vassilis, C. (2012). *Model security in cyber security systems*. International Journal of Critical Infrastructure Protection .5(3),118-126.

Camille M (2013), "Navigating the Telecom Cloud: Growth Perspectives," Informa Telecoms and Media (2013), http://www.informatandm.com/wp-content/uploads/2012/05/Informa-Telecom-Cloud-white-paper.pdf

Clayton, M. (2011, April 20) Security Lags Cyberattack Threats in Critical Industries, Report Finds. *CHRISTIAN SCIENCE MONITOR*. Retrieved from http://www.csmonitor.com/USA/2011/0420/Security-lags-cyberattack-threats-in-critical-industries-report-finds

Cockburn, A. & St. Clair, J. (1998) *Whiteout: The CIA, Drugs, and the Press.* New York: Verso.

Cooley, J. K. (2002). *Unholy Wars: Afghanistan, America, and International Terrorism.* Sterling, VA. Pluto Press.

Corera, G. (2013, Dec 1). "Spying Scandal: Will the 'Five Eyes' Club Open Up?" *BBC News*. Retrieved from http://www.bbc.co.uk/news/world-europe-24715168

Cornelius, R. (2011, Sept 13), "Deutsche Telekom Wants `German Cloud' to Shield Data From U.S." Bloomberg, Retrieved from http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html.14.

Croft, A, and Arshad, M. (2013 Dec 1) "France Summons U.S. Ambassador over Spying Report." *Reuters*. Retrieved from http://www.reuters.com/article/2013/10/21/us-france-nsa-idUSBRE99K04920131021

Duncan B. Hollis, (2011) *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373

Duncan B. Hollis, (2007) *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. REV. 1023, 1042.

Eisendrath, C. R. & Harkin, T. (2000) *National Insecurity: U.S. Intelligence After the Cold War*. Philadelphia, Pennsylvania. Temple University Press.

Entous, A. & Gorman S. (2013, Oct. 29) "U.S. Says European Helped NSA." *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502

Franklin, K. Larry, W. (2008).*International security and cyber influence*. Defense Horizons.61 (1),1-11.

Friedman, T. (2007) *The World Is Flat 3.0: A Brief History of the Twenty-First Century*. 3rd ed. New York, N.Y. Farrar, Straus and Giroux.

Gannon, J. (2001) *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century.* Washington, DC. Potomac Books, inc.

Gaouette, Nicole. (2013, Nov 26) "NSA Spying Risks $35 Billion in U.S. Technology Sales - Bloomberg." *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales.html

Gjelten, Tom. (2013, Nov 20) Profit, Not Just Principle, Has Tech Firms Concerned With NSA. *NPR.* Retrieved from http://wap.npr.org/news/U.S./246232540.

Gorman, S. (2010, June 4) U.S. Backs Talks on Cyber Warfare. *Wall Street*. Journal. Retrieved from http://online.wsj.com/news/articles/SB10001424052748703340904575284964215965730

Gragido, W., Pirc, J. & Rogers, R. (2011) *Cyber Crime and Espionage: An Analysis of Subversive Multi-Vector Threats*. Burlington, MA., Syngress.

Gray, J. A. (1984) *Theoretical sensitivity: Advances in the methodology of grounded theory* (Vol. 2). Mill Valley, CA: Sociology Press.

Greenberg, A.(2013, Nov 30). Intelligence Officials Admit That Edward Snowden's NSA Leaks Call For Reforms. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2013/09/13/intelligence-officials-admit-that-edward-snowdens-leaks-call-for-reforms/

Greenwald, G. (2013, July 31). "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet.'" *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Gup, T. (2001). *The Book of Honor: Covert Lives and Classified Deaths at the CIA.* New York, NY. Anchor Books.

Hastedt, G. P. *Spies, Wiretaps, and Secret Operations: An encyclopedia of American Espionage: Volume 1.* Santa Barbara, California: ABC-CLIO, LLC, 2011

Holmes, A. (2013, Sept. 10) "NSA Spying Seen Risking Billions Technology Sales." *Bloomberg.* Retrieved from http://www.bloomberg.com/news/2013-09-10/nsa-spying-seen-risking-billions-in-u-s-technology-sales.html

Hosenball, M. (2013, Nov 25) Spies Worry Over "Doomsday" Cacje Stashed by ex-NSA Contractor Snowden. *Reuters*. Retrieved from http://www.reuters.com/article/2013/11/25/us-usa-security-doomsday-idUSBRE9AO0Y120131125

Hulnick, A. S. (1999) *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century.* Westport, CT. Praeger.

Ing, N. & Jamieson, A. (2013, Nov. 7) NSA Spy Programs Show That 'America Doesn't Trust Its Allies', French Former PM Says. *NBC NEWS.* Retrieved from http://www.nbcnews.com/news/other/nsa-spy-programs-show-america-doesnt-trust-its-allies-french-f8C11549340

Jabeen, B. (2013, July 29), In Wake of PRISM, German DPAs Threaten To Halt Data Transfers to Non-EU Countries. *Bloomberg BNA*, Retrieved from http://www.bna.com/wake-prism-germann17179875502/.

Jeffreys-Jones, R. (2002). *Cloak and Dollar: A History of American Secret Intelligence.* New Haven, CT. Yale University Press.

Johnson, L. K. (2002). *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security.* New York: New York University Press.

Kalugin, O. (2009) *Spymaster : My Thirty-Two Years in Intelligence and Espionage Against the West*. New York, NY. Basic Books.

Kern, M. L. (2009) Statistical Methodology in Meta-Analysis.

Knightley, P. (1986) The Second Oldest Profession: Spies and Spying in the Twentieth Century, New York, NY. Penguin Books Edition.

Kramer, F. D. & Wentz, L. (2008). *International security and cyber influence*. Defense Horizons.61 (1),1-11.

Lee, Danny. (2013, July 9). "Snowden Tells of '5 Eyes' Spy Network, as Second Video from Hong Kong Interview Released." *South China Morning Post*. Retrieved

from http://www.scmp.com/news/world/article/1278285/snowden-tells-5-eyes-spy-network

Liptak, E. (2009) *Office of Strategic Services 1942-45: The World War II Origins of the CIA.* Oxford, UK. Osprey Publishing

Lowenthal, M. M. (2000). *Intelligence: From Secrets to Policy*. Washington, DC: CQ Press.

Lundestad, G. (2010). *East, West, North, South: Major Developments in International Politics Since 1945*. 6th ed. Thousand Oaks, California: SAGE Publications Inc.

MacDougal, M., Laswell, H. & Miller, J. (1994). *The Interpretation of International Agreements and World Public Order: Principles of Content and Procedure*. New Haven, CT. New Haven Press.

Malkin, B. (2013, June 9) "Edward Snowden: Defence Contractor Gives up 'Very Comfortable Life' to Blow Whistle on NSA Surveillance of Americans - Telegraph." *The Telegraph News*. Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10109460/Edward-Snowden-defence-contractor-gives-up-very-comfortable-life-to-blow-whistle-on-NSA-surveillance-of-Americans.html

Miller, S. P. (1999). *The Seventies Now: Culture as Surveillance.* Durham, NC: Duke University Press.

Nasheri, H. (2004). *Economic Espionage and Industrial Spying*. Cambridge, United Kingdom, The Press Syndicate.

Nye, J. S. (2011). *Nuclear Lessons in cyber security*. Strategic Studies Quarterly. 5(4), 18-38.

Office of the Director of National Intelligence (2011, Oct. 28). DNI Releases Fiscal Year 2011 Appropriated Budget Figure for the National Intelligence Program. *Office of the Director of National Intelligence*. Retrieved from http://www.dni.gov/index.php/newsroom/press-releases/97-press-releases-2011/328-dni-releases-fiscal-year-2011-appropriated-budget-figure-for-the-national-intelligence-program

Payne, E. & Shah, K. (2013, Oct. 21). Repot: U.S. Intercepts French Phone Calls on a 'Massive Scale.' *CNN*. Retrieved from http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/

Perry, C. (1998). A structured approach to presenting theses: notes for students and their supervisors. *Australasian Marketing Journal , (6* 1), 63-86

Petter,S.,Straub,D.,and Rai,A. (2007)"Specifying formative constructs in information systems research," MIS Quarterly (31:4),pp 623 656.

Poitras, Luara et al.(2013, July 1). "Secret Documents: NSA Targeted Germany and EU Buildings." Retrieved from http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html

Prodhan, G. & Davenport, C. (2013, June 7) US surveillance revelations deepen European fears. *Reuters*. Retrieved from http://www.reuters.com/article/2013/06/07/europe-surveillance-prism idUSL5N0EJ31S20130607

Rachael, K. (2013) The Wall Street Journal, NSA Spying Becomes Economic Issue for Tech Industry in 2012

Richards, J. (2009) "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." *International Affairs Review, Elliott School of International Affairs*. Retrieved from http://www.iar-gwu.org/node/65

Rogin, J. (2012, July 9) NSA Chief: Cybercrime Constitutes The "Greatest Transfer of Wealth in History. *The Cable.* Retrieved from http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history

Rolington, A. (2013). *Strategic Intelligence For The 21st Century: The Mosaic Method*. New York, N.Y.: Oxford University Press, 2013.

Sanchez, R. and Peter F. (2013, Oct. 29). "NSA Spy Row: France and Spain 'Shared Phone Data' with US." The Telegraph. Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10413260/NSA-spy-row-France-and-Spain-shared-phone-data-with-US.html

Sanger, D. E. & Smale, A. (2013,Nov. 11) "Spying Scandel Alters U.S. Ties With Allies and Raises Talk of Policy Shift. *The New York Times*. Retrieved from http://www.nytimes.com/2013/11/12/world/spying-scandel-alters-us-ties-and-raises-talk-of-policy-shift.html?_r=0

Sanger, D. E. & Smale, A. (2013, Dec 16) US-Germany Intelligence Partnership Falters over Spying, *The New York Times,* Retrieved from http://www.nytimes.com/2013/12/17/world/europe/us-germany-intelligence-partnership-falters-over-spying.html?hp&_r=1&

Saunders, M., Lewis, P. & Thornhill, A. (2009) Research methods for business students, 5th ed., Harlow, Pearson Education.

Shulsky, A. N. & Schmitt, G.J. (2002). *Silent Warfare: Understanding the World of Intelligence.* Washington, DC. Brassey's.

Singer, P. W., Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, Ny. Oxford University Press.

Smith, M. (2013, June 9). "NSA Leaker Comes Forward, Warns of Agency's 'Existential Threat' - CNN.com." *CNN*. Retrieved from http://www.cnn.com/2013/06/09/politics/nsa-leak-identity/

Srodes, J. (1999) *Allen Dulles: Master Spies.* Washington DC. Regnery Publishing Inc.

Supinski, S. (2013, Oct. 30) "France 'Spied on French Phones for the US.'" *The Local: France's News in English*. Retrieved from http://www.thelocal.fr/20131030/france-spied-on-french-phones-for-the-us

Theoharis, A. (2002) *Chasing Spies: How the FBI Failed in Counterintelligence but Promoted the Politics of McCarthyism in the Cold War Years.* Chicago, IL. Ivan R. Dee.

Theoharis, A. (2011) Abuse of Power: How Cold War Surveillance and Secrecy Policy Shaped the Response to 9/11. Philadelphia, Pennsylvania. Temple University Press

Todd, T. (2013, Oct. 26) "Paris Also Snoops on US, Says French Former Spy Boss." *France 24*. Retrieved from http://www.france24.com/en/20131024-nsa-france-spying-squarcini-dcri-hollande-ayrault-merkel-usa-obama/

Treverton, G. F. (2003) *Reshaping National Intelligence for an Age of Information.* New York: Cambridge University Press.

Treverton, G. F. (2002) *Chasing Spies: How the FBI Failed in Counterintelligence but Promoted the Politics of McCarthyism in the Cold War Years.* Chicago: Ivan R. Dee, 2002.

United Nations Centre (2013, Sept 24) "United Nations News Centre - At UN Debate, Brazilian President Urges Protection of Internet Users." *UN News Centre*. United Nations. Retrieved from http://www.un.org/apps/news/story.asp?NewsID=45955#.VAt-O2MiPMQ

United Nation General Assembly (2013, Nov. 26) "Third Committee Approves Text Titled 'Right to Privacy in the Digital Age'." *United Nations.* Retrieved from *http://www.un.org/News/Press/docs//2013/gashc4094.doc.htm.* United Nations, November 26, 2013)

US Department of State (2014) "Under Secretary for Public Diplomacy and Affairs", US *Department of State.* Retrieved from http://www.state.gov/r/

Vida A (2008), *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 Naval L. REV. 132, 140.

Watts, J. (2013, Sept. 9) "NSA Accused of Spying on Brazilian Oil Company Petrobras." The Guardian. Retrieved from http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

Webb, G. (1998) *Dark Alliance: The CIA, the Contras, and the Crack Cocaine Explosion.* New York: Seven Stories Press.

Weiner, T. (2008) *Legacy of Ashes: The History of the CIA*. New York, NY. Anchor Books

William H. (2010, May 22) DoD Cyber Command Is Officially Online, *ARMY TIMES* (May 22, 2010), Retrieved from http://www.armytimes.com/article/20100521/NEWS/5210319/DoD-Cyber-Command-officially-online

Wilson, M. (2010). The retooled mind: How culture re-engineers cognition. *Social, Cognitive, and Affective Neuroscience,* doi:10.1093/scan/nsp054

Zegart, A. B. (1999) *Flawed by Design: The Evolution of the CIA, JCS, and NSC.* Stanford, CA: Stanford University Press.

Zhou, G., Wang, D. W., Li, F., Zhang, L., Li, N., Wu, Z. S., ... & Cheng, H. M. (2010). Graphene-wrapped Fe3O4 anode material with improved reversible capacity and cyclic stability for lithium ion batteries. *Chemistry of Materials*, *22*(18), 5306-5313.

BIOGRAPHY

Cliffard A. Patton received his adult education certificate at a Brevard County, Florida institution in 2002. He received his Bachelor of Arts and Bachelor of Science degrees from Florida State University in 2012. He then received his Master of Science in Conflict Resolution and Mediterranean Security from the University of Malta in 2014 and his Master of Arts in Conflict Analysis and Resolution from George Mason University in 2015.