ESPIONAGE: A COMPARATIVE ANALYSIS

Kristin A. Vara

I. INTRODUCTION ........................................... 61
II. ESPIONAGE: A HISTORY .................................. 63
III. CURRENT CASES IN THE UNITED STATES AND RUSSIA .... 66
   A. Two of the Three Russian Spies in New York... 66
      Evade Prosecution .................................... 66
   B. Alleged CIA Agent Caught Spying in Russia ... 68
   C. Ten Russian Sleeper Agents Discovered, Yet Successfully Traded for American Prisoners .... 68
IV. KEEPING FRIENDS CLOSE AND POTENTIAL ENEMIES CLOSER .... 70
V. ANALYSES OF RUSSIA'S ESPIONAGE TACTICS AND LAWS .... 71
   A. Russia's Foreign Intelligence Agencies and Operations .... 71
   B. Russia's Laws Regarding Foreign Intelligence .... 73
VI. ANALYSES OF THE UNITED STATES' ESPIONAGE TACTICS AND LAWS .... 76
   A. The United States' Foreign Intelligence Agency and Operations .... 76
   B. The United States' Laws Regarding Foreign Intelligence .... 80
VII. COMPARISON OF HOW SPIES ARE PROSECUTED IN THE UNITED STATES AND RUSSIA .... 85
VIII. LEGAL ANALYSES OF LAWS RELATING TO ESPIONAGE IN THE UNITED STATES AND RUSSIA .... 86
IX. CONCLUSION ........................................... 89

I. INTRODUCTION

"Espionage is as pervasive today as it has ever been." When one thinks of espionage, thoughts of covert operations and Cold War tactics often come into play. Many might even believe that espionage—or spying as it is sometimes referred— is just a thing of the past. That could not be further from the truth. In recent years, the United States has dealt with numerous

* Kristin A. Vara, Bachelor of Science in Criminology from Florida State University in 2014, Nova Southeastern University Shepard Broad College of Law Class of 2017. Special thanks to my father and mentor, Daniel N. Vara, Jr., for both the inspiration and encouragement.

instances of espionage, and although not as glamorous as some would think, it is evidence of the continuation of a tactic that dates back centuries.  

My purpose in choosing this topic is to explore and expose the continuing espionage effort between the United States and Russia. The Cold War is decades in the past. Yet, in reality, not as much has changed as many would believe. This article will therefore discuss not only the instances of espionage between the two countries, but also the laws related to espionage in each country and the difficulties surrounding the prosecution of known or alleged spies.

Specifically, I chose to address this subject to enlighten, compare, and contrast between the types of laws that are used in both the United States and Russia to seek to combat and address foreign espionage, and the difficulties each country faces when weighing all the involved variables and deciding what recourse to take.

The first section of this article will begin with a history of espionage in the United States and Russia, and an explanation of how espionage came to be utilized by each country, primarily, against the other.

The second section of this article will address three recent cases involving the United States and Russia concerning espionage and spy tradecraft activity.

This section of the article will also provide background into the structure of the Russian government and the intelligence agencies that operate within, followed by an explanation of the laws that Russia uses to handle known or suspected spies. It will then provide an overview of the structure of the United States government and the American agencies that are responsible for handling intelligence and espionage. This will be followed by a presentation and exploration of the laws employed in the United States when dealing with known or suspected foreign intelligence agents working on American soil and/or against the homeland.

This will allow a comparison of the two countries and how their counter-intelligence systems, laws, and methods differ and how they are similar.

The third and final section of this article will conclude with my opinion about why some of the laws employed seem to be more effective than others. Further, it will explain the problems surrounding criminal prosecution of alleged spies in both the United States and Russia. Lastly, this article will summarize the information shared and give my opinion on what changes should and could be made in this area of law.

2. Id.
II. Espionage: A History

In the late 1930s the Federal Bureau of Investigation ("FBI") began uncovering a new wave of evil that had surfaced—spies. These secret agents were sent into the United States under the authority of their various fascist dictators and fanatical militarists to uncover sensitive information that would aid in their mission to conquer the world. These Nazi tactics had the government concerned for the welfare of the people and democracy itself, leading President Roosevelt to take action.1

In 1934, as suspicions about the Nazi Party of the United States and other similar groups’ loyalties grew, President Roosevelt had the FBI look into these American Nazi affiliations in an attempt to determine if they were working as foreign agents.2 Two years later the FBI gained the responsibility of gathering intelligence on all national security threats posed by fascist groups.3 During such time, espionage at the hands of the German Nazis and the Japanese, who had now aligned themselves with Germany as part of the Axis Powers at war with the world, had soared to new heights, giving the Bureau a new wave of spies to search for.4 These investigations led the FBI to discovering almost fifty spies in this country by the time America entered the war.5

By 1940, President Roosevelt had FBI agents undercover as champion golfers, traveling companions, and friendly visitors to foreign nations, particularly South and Central America, as part of a "Special Intelligence Service."6 This was due to South America having become an immigration hot-spot for more than half-a-million Germans, many of whom were supporters of the Nazi’s.7 Within the next seven years, the FBI had more than 340 agents and undercover support staff in South and Central America gathering intelligence information on Nazi activity as part of the Special Intelligence Service.8

4. id.
5. id.
6. id.
7. id.
8. World War, Cold War, 1939-1955, supra note 3.
9. id.
10. id.
11. id.
12. id.
The results were fruitful to say the least. By 1946, these American agents had identified “877 Axis spies, 281 propaganda agents, 222 agents smuggling strategic war materials, 30 saboteurs, and 97 other agents.”13 In addition, these agents were able to uncover 24 secret Axis radio stations and confiscate 40 radio transmitters as well as 18 receiving sets.14

During World War II, Russia, referred to as the Soviet Union, and the United States became allies, fighting against Nazi Germany.15 Russia, among many other countries, was given millions of dollars’ worth of weapons and other supplies to aid in their fight against Nazi Germany through the Lend-Lease program.16

In these early stages of the American counter-intelligence effort, the United States had not been primarily focused on possible Russian espionage.17 But then, an anonymous letter was sent to FBI Headquarters in the summer of 1943.18 This letter contained a series of accusations of espionage activities by more than ten Russian diplomats; accusations which were hard to fathom on the part of United States intelligence and the administration since the Russians had ostensibly been and continued to be our allies.19 Yet, the United States was already two steps ahead, as the FBI had already begun gathering information on Soviet Intelligence.20

In fact, four months before receiving the letter, the FBI had gathered information that the Communist party had sought to infiltrate a California lab that was working on the Manhattan Project, America’s clandestine atomic bomb program.21 During this time Russia had used spies to infiltrate the United States and gain intelligence on the secrets of nuclear war.22 This discovery led the Bureau to looked deeper into Soviet espionage—thankfully so—as it was not only a huge problem but also a huge threat.23

However unpleasant as some of these discoveries might have been to this country’s authorities, they served as precursor events that prepared the

13. World War, Cold War, 1939-1953, supra note 3.
14. Id.
17. World War, Cold War, 1939-1953, supra note 3.
18. Id.
19. Id.
20. Id.
21. Id.
22. History of America- USA vs. Russia, HISTORY.COM http://www.history.co.uk/study-topics/history-of-america/usa-vs-russia (last visited July 30, 2015) [hereinafter History of America].
23. World War, Cold War, 1939-1953, supra note 3.
FBI and entire United States intelligence apparatus for what was to come in the Cold War.\textsuperscript{24}

By the time World War II was over, the Russians had several of their intelligence agents in sensitive positions in our government, to include some intelligence positions.\textsuperscript{25} This infiltration had clearly done damage to national security.\textsuperscript{26} By 1948, stories about Russian spies littered the front pages of newspapers and magazines across the country, incriminating even well-known attorneys for having passed along sensitive information to the Russian government.\textsuperscript{27}

In response, the United States government was quick to act and, in earnest, began to dismantle the Russian spy networks with the help of their allies, Canada and Great Britain.\textsuperscript{28} Ultimately, it was the top secret Project Venona, which ran from 1943 to 1980, that helped the United States identify approximately 350 people connected to Soviet intelligence through decoding Soviet cables.\textsuperscript{29}

The FBI efforts proved fruitful in discovering and shutting down many Soviet moles and double agents, foreign agents who managed to covertly infiltrate the United States government and its secrets while working on behalf of and against America, who betrayed the United States and were in fact working for a foreign power.\textsuperscript{30} By the early 1950s, the Russian’s regrouped and began sending in “illegal” agents who were to gather intelligence while remaining under various covers.\textsuperscript{31} The Soviets continued using these spies throughout the remainder of the Cold War and still continue to use such covert agents today.\textsuperscript{32}

Thus, it is a fallacy that the contest between the United States and Russia ended with of the Cold War, as both continue to send and keep spies into the others’ country in order to obtain sensitive and highly classified information.\textsuperscript{33}

\begin{thebibliography}{99}
\bibitem{24} "\textsuperscript{24} Id.
\bibitem{25} Id.
\bibitem{26} Id.
\bibitem{27} Id.
\bibitem{28} Id.
\bibitem{29} Id.
\bibitem{30} Id.
\bibitem{31} Id.
\bibitem{32} Id.
\bibitem{33} Id.
\end{thebibliography}
III. CURRENT CASES IN THE UNITED STATES AND RUSSIA

A. Two of the Three Russian Spies in New York Evade Prosecution

One of the most recent cases to date dealing with espionage discovered within the United States became public knowledge on January 26, 2015, when Russian intelligence agents Evgeny “Zhenya” Buryakov, Igor Sporyshev, and Victor Podobnyy were arrested in connection with a Russian spy ring.34 Buryakov, Sporyshev and Podobnyy were sent to the United States to recruit spies for Russia and to engage in intelligence gathering activities in the New York City area.35 Some of the tasks assigned to the group included gathering intelligence on classified economic issues, alternative energy, and potential sanctions against Russia.36 Specifically, Buryakov had been tasked with attempting to recruit United States residents as spies for Russia, including people employed for major American companies and universities.37

Buryakov had been in disguise as a low level employee in a Manhattan Russian bank, but in actuality was a Russian intelligence agent under non-official cover (“NOC”), which allowed him to operate as an employee of a private business.38 One might think that a secret agent under NOC would be ineffective due to the potential limitations of living a completely covert life without direct and easy access to their country’s resources.39 However, NOCs are very valuable by the very nature of their methods of operation, as they are not readily known to the host governments. Thus, they do not have the typical limitations of agents with official cover whose activities are constantly monitored by the United States and other intelligence services.40

Despite his cover as a NOC, the FBI had been aware of Buryakov for some time before his arrest on January 26, 2015.41 Since 2012, FBI Special Agent Gregory Monaghan and other law enforcement agents had been

36. Vicinanzo, supra note 1.
37. *Id.*
38. *Id.;* Buryakov et al., at 4.
39. Vicinanzo, supra note 1.
40. *Id.;* Buryakov et al., at 4.
41. Vicinanzo, supra note 1; Buryakov et al., at 2.
conducting an investigation that included video and electronic surveillance on Buryakov, Sposhysh and Podobnyy.

Between March 2012 and September 2014, over four dozen quick meetings between Buryakov and two other operatives were recorded on physical surveillance in addition to a recorded conversation that occurred in May 2013.

Coded messages led to secret meetings that consisted of sharing documents and other small items—such as an umbrella or a ticket—that contained intelligence-related information. These meetings usually occurred outdoors as surveillance risks lower. The FBI gained knowledge of these events through physical and electronic surveillance that included the covert placement of video cameras and microphones in public locations, phone tapping, and confidential sources.

As Sposhysh served as the Trade Representative of the Russian Federation in New York and Podobnyy served as an Attaché to the Permanent Mission of the Russian Federation to the United Nations, they were both exempt from the registration requirement. Although both Sposhysh and Podobnyy were not required to register, both were in violation of 18 U.S.C. § 2 for being a principal to a crime and 18 U.S.C. § 371 for conspiring with Buryakov to violate 18 U.S.C. § 951, as an unregistered agent of a foreign government. Regardless of these violations, Sposhysh and Podobnyy were both no longer residents of the United States at the time of the arrest and were protected by diplomatic immunity from arrest and prosecution while in the United States.

Buryakov, however, was not so fortunate. He was arrested and criminally charged under 22 U.S.C. § 951 for failing to notify the Attorney General that he was working as an agent for Russia amongst other criminal charges.

42. Buryakov et al., at 1-3.
43. Victorino, supra note 1, Buryakov et al., at 2.
44. Victorino, supra note 1, Buryakov et al., at 7.
45. Victorino, supra note 1, Buryakov et al., at 7.
46. Buryakov et al., at 6.
47. Id. at 5.
48. Id.
49. Victorino, supra note 1.
50. Buryakov et al., at 2
B. Alleged CIA Agent Caught Spying in Russia

Conversely, on May 14, 2013, the Russian authorities arrested an alleged CIA agent named Ryan Fogle, who had been working as a third secretary at the United States Embassy in Moscow. Fogle, while working in the lowest entry level position in the Foreign Service, was accused of attempting to recruit a member of the Russian Secret Service to work as an agent for the United States.

Fogle was reported to have been charged with attempting to recruit a counter-terrorism officer with specialization in the Caucasus, where the Boston Marathon Bombers are said to trace their lineage. Technical equipment, disguises, money, and instructions were found on Fogle when he was taken into custody of the Russian government.

Based on diplomatic immunity, Fogle was subsequently released and ordered to leave Russia immediately as a persona non grata, or unwelcome person. Fogle was the first American diplomatic employee accused of spying in almost a decade.

Since both the CIA and the United States Ambassador to Russia declined to comment on this case, it is still a mystery whether Fogle was a United States intelligence agent or a man caught up in a series of unfortunate events.

C. Ten Russian Sleeper Agents Discovered, Yet Successfully Traded for American Prisoners

A third recent espionage story involving Russia surfaced on June 27, 2010, when the United States agreed to exchange ten known Russian spies for four Russians who had been imprisoned for years due to their contacts.

---

52. Id.
53. Id.
54. Id.
55. Id.
56. Russia claims CIA agent arrested, supra note 51.
57. Id.
with the West. The ten Russian spies were disguised as married couples who lived in the suburbs and raised children together for over a decade. These agents had assumed covers as a professor, newspaper columnist, and an architect, among other things.

In actuality, these Russian agents were passing along information to the Moscow Center using high tech computer networks and tools such as invisible ink, and tactics such as trading bags in the train station. These agents were not actively seeking classified information and were instead “slower agents”—spies who are placed into a particular location not to act immediately, but to be ready to act when needed.

Among the ten arrested was the well-known Anna Chapman, who has become an icon of the media version of the young, attractive Russian spy. The United States’ investigation into these ten spies revealed that they had taken the identity of deceased persons in efforts to falsify legal documents and further their undercover efforts. Their mission, as discovered by the FBI through decryption of coded messages sent by Moscow Center to the defendants, was “to search and develop ties in policymaking circles in the United States and send Intel [intelligence reports] to Moscow Center.”

Uncovering these spies did not come easily and instead was the result of a multi-year FBI investigation. These foreign agents were part of the “illegals” program and were sent to the United States under “deep cover,” with instructions to hide all connections they had with Russia.
the defendants pleaded guilty to spying and all ten were subsequently deported in what came to be the "largest prisoner swap since the Cold War."68

Although removal of the agents via a trade between the United States and Russia was the end result, the arrests of the Russian agents were not effectuated with the intention of seeking out a trade.69 That was determined after their arrest, upon United States officials learning that these agents were unsuccessful in infiltrating United States intelligence. It would better serve America to use these agents as a way to regain American assets that had been confiscated by Russia for years.70

Ultimately, the United States got everything it asked for as a result of the trade, as they were able to regain the four prisoners and establish an agreement that Russia would not take any retaliatory steps against the United States.71

IV. KEEPING FRIENDS CLOSE AND POTENTIAL ENEMIES CLOSER

Although it may seem as though instances of espionage only occur between nations with adverse relations, that is not the case. Even those nations that are allies are known to still make use of spy tactics to obtain information about one another.72 This is because, as experts say, "a friend today may not be a friend tomorrow."73 For example, the United States received criticism a few years ago when it was discovered that they were spying on the German Chancellor, Angela Merkel’s, cell phone.74

However, the United States is not apologizing. The United States’ Director of National Intelligence said that it is fundamental, given that the United States spies on foreign leaders.75 This is because mutual spying even among friendly countries is a common and quietly accepted practice that most nations engage in.76

69. Id.
70. Id.
71. Id.
72. Id.
73. Id.
74. Id.
75. Id.
76. Martinez, supra note 73.
V. ANALYSIS OF RUSSIA’S ESPIONAGE TACTICS AND LAWS

A. Russia’s Foreign Intelligence Agencies and Operations

Like the United States, Russia has a department whose primary responsibility is to collect and protect intelligence. The Foreign Intelligence Service ("SVR") is the name of what used to be the KGB (Committee of State Security in Russia) until 1991. The SVR employs approximately 13,000 personnel who are responsible for protecting Russia’s security systems from external threats. The SVR works in tandem with Russian Military Intelligence ("GRU"), and has its own academy for training recruits.

Additionally, Russia has the Federal Security Service ("FSB"), which was established in 1994. This agency shares many similarities with the FBI and is responsible for coordinating counter-intelligence efforts of other federal bodies, including anti-terrorism responsibilities, counter-intelligence, and surveillance of the Russian military. The FSB is believed to be Europe’s largest security service, with approximately 75,000 employees as of 2016.

In the complaint against eight of the ten Russian spies arrested June 27, 2010, the United States government outlined operations, strategies, and methods descriptive of how Russia trains its spies. The complaint asserts that secret agents who are sent under deep-cover to a foreign nation are often referred to as "illegals." These agents receive a high degree of training in areas such as foreign languages, agent-to-agent communications, including the use of brush-passes, short-wave radio operation and invisible

79. Id.
80. Id.
83. "Federal Security Service, supra note 81; Threat Handbook, supra note 82, Russia’s SVR agency, supra note 78.
84. Id., at n.6.
85. Id.
writing; the use of codes and ciphers, including the use of encrypted Morse code messages; the creation and use of cover profession, counter-surveillance measures, concealment and destruction of equipment and materials used in connection with their work as agents; and the avoidance of detection during their work as agents.\textsuperscript{86}

The complaint added that Russian illegals also received false identities, along with coordinating falsified documents to create what is referred to as their "legend".\textsuperscript{87} The illegals are then sent to various countries disguised as residents of that nation.\textsuperscript{88} At times, illegals are placed together in operations, and when that occurs, the agents will often have children together in an attempt to further solidify their cover.\textsuperscript{89}

The complaint also contained descriptions of various methods Russia uses for secret communications. The first is a "brush pass," or "flash meeting," in which a secret delivery of items or money is made as two people walk past one another in public.\textsuperscript{90} The second tool used is steganography, which is the process of placing a secret encrypted image on a public website.\textsuperscript{91} The receiver then removes the image from the website using a specialized software that decrypts the message.\textsuperscript{92}

A third method used are radiograms, which are coded data sent through a radio transmitter and picked up on another radio if tuned to the correct frequency.\textsuperscript{93} Radiograms usually resemble the sound of Morse code transmissions.\textsuperscript{94}

In the complaint against the three alleged spies arrested this year in New York, FBI agent Gregory Monaghan explained how SVR foreign agents operate.\textsuperscript{95} Monaghan indicated that there are three categories of SVR foreign agents.\textsuperscript{96} The first class are sent to various countries in deep cover, where

\textsuperscript{86} Id. at 4-5
\textsuperscript{87} Id.
\textsuperscript{88} Id.
\textsuperscript{89} Metsos et al., at 4-5.
\textsuperscript{90} Id. at 4
\textsuperscript{91} Id. at 9
\textsuperscript{92} Id.
\textsuperscript{93} Id. at 11.
\textsuperscript{94} Metsos et al., at 11.
\textsuperscript{96} Id.
they have disguises, work regular jobs, and attempt to hide all connections with Russia. 97

SVR’s second class consists of agents that do not assume an undercover position and are sent abroad to pose as Russian representatives. 98 These agents are often given diplomatic immunity from prosecution if they are caught. 99 Diplomatic immunity is international law that requires authorities in various countries to “extend privileges and immunities to members of foreign diplomatic missions and consular posts.” 100

The third class of SVR foreign agents are NOCs, which are those under non-official cover in the host country. 101 These agents are typically abroad and pose as private business employees. 102 Often times these agents are not the subject of a high degree of scrutiny by their host government and are sometimes never even identified as foreign intelligence agents. 103

Although there are significant differences in the way each agent classification works, the singular goal remains the same: to infiltrate the infrastructure of whatever foreign country they are in and obtain useful information to relay back to Russia. 104

B. Russia’s Laws Regarding Foreign Intelligence

The Criminal Code of the Russian Federation lays out all of the criminal laws of Russia. 105 Section ten deals with “Crimes against State Power.” 106 There are three main articles that deal with treason, espionage, and the disclosure of state secrets. 107

Article 275 deals with what is termed “High Treason,” which is “espionage, disclosure of state secrets, or any other assistance rendered to a foreign State, a foreign organization, or their representatives in hostile

97. Id.
98. Id.
99. Id.
101. Bender, supra note 95.
102. Id.
103. Id.
104. Id.
105. УК РОССИЙСКОЙ ФЕДЕРАЦИИ [UK RF] (Criminal Code) (Russ.).
106. Id. at sec. 1.
107. Id.
activities to the detriment of the external security of the Russian Federation, committed by a citizen of the Russian Federation."

Under Article 275, High Treason is punishable by twelve to twenty years imprisonment and/or a fine of up to 500,000 rubles, or two years imprisonment and a fine of the wages, or other income of the convicted person for up to three years.

Article 276 relates to espionage and sets forth that the transfer, collection, theft, or keeping protected information:

for the purpose of transfer to a foreign state, a foreign organization, or their representatives of information constituting a state secret, and also transfer or collection of other information under the order of a foreign intelligence service, to the detriment of the external security of the Russian Federation, if these deeds have been committed by a foreign national or stateless person [is espionage].

Espionage is punishable by imprisonment from ten to twenty years under this article.

Article 283 regards the "Disclosure of State Secrets." Disclosing a state secret is punishable "by arrest for up to four years, or by deprivation of liberty for up to four years, with disqualification from holding specific offices or engaging in specified activities" for up to three years, or without being disqualified in such a way. One is guilty of this crime if they disclose information that comprises a "state secret, by a person to whom it has been entrusted or to whom it has become known through his office or work, if this information has become the property of other persons, in the absence of the characteristic features of high treason."

In 2012, amendments were made to the three above-mentioned articles of the Criminal Code. Law No. FZ-190 was adopted on October 23, 2012
by the State Duma. This law expanded the definitions of the terms "treason" and "espionage" in the Russian Criminal Code.

Under Article 275 dealing with treason, this law added additional actions, subjects, and situations that constitute treason. The law makes consulting or assisting a foreign state, an international or foreign organization, or any of their representatives in ways that would be adverse to the security of the Russian Federation, an act of treason. Additionally, the law expands the list of covered circumstances in which a Russian citizen could have obtained protected state secrets from "service and work" to "study or other cases."

The new law also expanded the list of international organizations to which transferring a state secret would be considered treason.

In regards to the term treason, FZ-190 state treason was changed from actions against the "external safety of the Russian Federation" to actions against "the security of the Russian Federation." FZ-190 further amended Article 276 regarding espionage by expanding the meaning of the term in several ways. For instance, the amended article expanded the meaning of the term by no longer requiring an order from a foreign intelligence service for the transfer of information that does not constitute a state secret that will be used against Russian security by a stateless person or a foreign national to be considered espionage. Beyond that, various international organizations are now considered covered entities to which the transfer of protected information is deemed punishable under the act.

This amendment also made changes to Article 283 by adding two new sections. The first section makes it a crime to obtain information that is a state secret through abduction, deception, blackmail, threatened violence,
coercion, or other illegal means. A person found in violation of this article will be punished by receiving a fine ranging from 200,000 to 500,000 rubles or “in the amount of the wages or salary or any other income of the convicted person for a period from one to three years, or by deprivation of liberty for a term up to four years.”

Finally, if that same act is committed by a group that used violence, caused grave consequences, was committed with the use of special or surreptitious means of obtaining the information, and is connected with the dissemination of information that is a state secret or brings that information outside the borders of the Russian Federation, then they are in violation of the article and can be punished by imprisonment from three to eight years.

These three articles of law, and the noted subsequent amendments, are the three most frequently used laws in Russia when dealing with potential or known instances of espionage or the sharing of state secrets.

VI. ANALYSIS OF THE UNITED STATES’ ESPIONAGE TACTICS AND LAWS

A. The United States’ Foreign Intelligence Agency and Operations

On July 11, 1941, five months prior to the bombing of Pearl Harbor, President Franklin D. Roosevelt established the Office of the Coordinator of Information, giving it the responsibility of organizing the intelligence activities of various agencies.

In June of 1942, the Office of Strategic Services (“OSS”), which is the predecessor of today’s Central Intelligence Agency (“CIA”), was created as a result of and in reaction to the bombing of Pearl Harbor. The OSS’ mission was to conduct specialized assignments and to collect and analyze information mandated by the Joint Chiefs of Staff.

127. Id.
128 One United States dollar is the equivalent of 54.81 Russian Ruble’s; therefore, in United States currency the fine for being found in violation of these articles ranges from $3,648.96 to $9,122.42. See Exchange Rates from USD to RUB, GOOGLE, https://www.google.com/search?q=rubles+to+usd+money+convert&aqi=maps&as_qrc=chrome..69557.39859&source=chrome&esp=93&ie=UTF-8&ie=UTF-8&aqi=maps&as_qrc=chrome..69557.39859&source=chrome&esp=93&ie=UTF-8 (last visited September 26, 2015).
129. Id.
130. Id.
133. Id.
When Harry S. Truman became president in 1945, he abolished the OSS and divided its responsibilities among other agencies. However, President Truman ultimately realized the need for a dedicated primary intelligence agency, which led to the establishment of the Central Intelligence Group (CIG) in January of 1946. The CIG had two main goals: "to provide strategic warning and to conduct important clandestine activities." Within twenty months, the CIG was abolished and the CIA was established under the National Security Act of 1947.

Since that time, the CIA has been the United States’ premiere spy agency. The mission of the CIA is to collect and analyze intelligence obtained from or about other countries and share this information with other governmental agencies for the purpose of advancing this country’s national security interests.

In 1952, with the advancements in signals and electronic communications, the National Security Agency ("NSA") was created to intercept and decode foreign communications as well as seek and ensure that hackers, who are unable to gain sensitive information about the United States.

In March 2014, the CIA announced that it is creating a new division to combat cyber-espionage called the Directorate of Digital Innovation. This new department is being created to help the CIA develop the specialized skills, programs, and tactics that will allow them to trace the digital trail of potential spies.

Finally, the CIA has announced that it will be restructuring the way it teaches spy craft, shifting from individual schools and training programs, to an all-inclusive training facility called the "CIA University."
The United States also has highly sophisticated counter-intelligence agencies within the Department of Justice that are subcategorized under the National Security Division ("NSD"). See chart below.

The Counter-intelligence and Export Control Section handles all investigations and prosecutions of cases that relate to national security. This division is responsible for the oversight of eighty-eight federal statutes that deal with national security, one of the many being espionage. This division provides information to United States Attorneys and investigative agencies across the country regarding information found within their areas of responsibility which aid in the prosecution of violators and those deemed to pose a threat to national security. Additionally, this section coordinates the requirements of and compliance with the Classified Information Procedures Act ("CIPA"), Foreign Agents Registration Act ("FARA"), and

146. Sections & Offices, supra note 144.
147. Id.
148. Id.
other sensitive national security information disclosure statutes in criminal cases.\textsuperscript{149}

Since September 11, 2001, the NSD’s Office of Intelligence has significantly expanded to ensure that the intelligence community has the continuing legal authority to conduct operations, specifically the operations involving the Foreign Intelligence Surveillance Act.\textsuperscript{150}

Another vital section of the National Security Department is the Operations Section, whose role is to represent the government in cases before the Foreign Intelligence Surveillance Court ("FISC").\textsuperscript{151} This department deals mainly with the preparation and filing of all documentation related to the FISA.\textsuperscript{152} This division is sub-divided into three parts, each ensuring in a different way that the United States has the tools and the legal authority necessary to successfully prosecute these cases. The sub-divisions are (1) the Counter-terrorism Unit, (2) the Counter-intelligence Unit, and (3) the Special Operations Unit.\textsuperscript{153} Beyond its legal staff, this department of the NSD additionally employs intelligence research specialists who belong to a specialized unit called the Classified Information Management Unit.\textsuperscript{154} The Operations Section works with the Oversight Section on tasks such as sharing information among the United States Intelligence community and the distribution of other FISA-related insights and information.\textsuperscript{155}

As noted, within the National Security Department is another unit, the Oversight Section.\textsuperscript{156} This section provides the very important function of overseeing and monitoring intelligence and national security related activities by the governmental agencies of the United States to ensure that activities are in compliance with the Constitution and federal statutes.\textsuperscript{157} One of the more crucial functions this department has is weighing the need of the government to gather foreign intelligence with the need to protect the privacy of society and the civil liberties we are entitled to.\textsuperscript{158} In order to properly monitor the compliance of all on-going intelligence activity, the Oversight

\textsuperscript{149} Id.

\textsuperscript{150} Id.


\textsuperscript{152} Id.

\textsuperscript{153} Id.

\textsuperscript{154} Id.

\textsuperscript{155} Sections & Offices, supra note 144.


\textsuperscript{157} Id.

\textsuperscript{158} Id.
Section prepares a plethora of reports to indicate progress, compliance, and non-compliance.159

A fourth section in the National Security Department is the Litigation Section.160 This department was developed as a result of the increasing need for coordination between intelligence and law enforcement personnel regarding to the Foreign Intelligence Surveillance Act and the investigations and prosecutions of spies and terrorists.161 In creating this department, the government’s goal was to ensure that the National Security Department had resources available to prosecutors that would help them handle evidentiary and discovery related issues pertaining to FISA cases.162

The fifth office of the National Security Department is the Executive Office.163 This division is responsible for a number of support functions to the NSD Sections and Offices such as training, procurement services, telecommunications, and finance and travel services.164

Lastly, the Law and Policy Office is responsible for the implementation of policies concerning intelligence, counter-terrorism and other issues pertaining to national security.165 This office is also tasked with being the legal advisors to the Director of National Intelligence on all matters pertaining to national security law.166

B. The United States’ Laws Regarding Foreign Intelligence

There are a variety of laws in the United States that deal with espionage in various contexts. Federal prosecutors utilize particular statutes over others depending on the particular facts of each case and the statute that will impose the least burdensome test for the prosecution.

One law denies entry into America for any alien whom the Attorney General or a consular officer knows or reasonably believes is seeking entry into the United States with the purpose of violating any laws of the United States as it relates to espionage or sabotage.167 Another law makes any alien who is engaged in, has engaged in, or, who any time after gaining entry into

159. Id.
161. Id.
162. Id.
163. Id.
164. Id.
165. Sections & Offices, supra note 144.
166. Id.
the United States, engages in any act or acts that violate laws pertaining to espionage or sabotage, subject to deportation.

One of the frequently utilized laws the United States government uses to combat espionage is the Foreign Agent Registration Act of 1938. This act was adopted in response to pre-Nazi activities within the United States. The act, which has been updated since its enactment, states that

Chapter 11, § 611 of the act provides the definition of the term "agent of a foreign principal." Under Chapter eleven, an "agent of a foreign principal" is any person who acts as an agent, representative, employee, or servant, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign principal or of a person any of whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in part by a foreign principal, and who directly or through any other person engages within the United States in political activities for or in the interests of such foreign principal acts within the United States as a public relations counsel, publicity agent, information service employee or political

170. Id.
consultant for or in the interests of such foreign principal; within the United States solicits, collects, disburses, or dispenses contributions, loans, money, or other things of value for or in the interest of such foreign principal; or within the United States represents the interests of such foreign principal before any agency or official of the United States; and any person who . . . holds himself out to be . . . an agent of a foreign principal. 173

However, this law excludes news or press service employees or associations that were organized under United States laws from having to register if they meet certain qualifications. 174

Another act utilized is a registration act of Certain Persons Trained in Foreign Espionage Systems, which was enacted in 1956. 175 Under this statute, "every person who has knowledge of, or has received instruction or assignment in, the espionage, counter-espionage, or sabotage service or tactics of a government of a foreign country or of a foreign political party, shall register with the Attorney General." 176

Additionally, 18 U.S.C. § 951 requires that anyone acting in the United States as an agent of a foreign government shall register with the Attorney General, unless they are a diplomat, consular officer or attaché. 177

In 1996, the United States enacted a law titled Gathering and Delivering Defense Information to Aid Foreign Government, that made it illegal to deliver, transmit, communicate, attempt to communicate any code book, signal book, writing, document, sketch, blueprint, photograph, photographic negative plan, note, model, instrument, appliance, or any information to a foreign nation, representative, or citizen thereof with the intent or reason to believe that the information will be used to injure the United States. 178 Violation of this statute is punishable by death or imprisonment for any number of years to include life. 179

Based on the nuances and complexities of the laws applicable to espionage activities, the criminal prosecution of alleged spies has proven difficult for the United States government. The United States often makes use of immigration law to deal with known or suspected spies, and has even used the immigration law model as the predicate for the criminal prosecutions

173. _Id._
174. _Id. at (6)._ 175. 50 U.S.C. § 851 (1956).
176. _Id._
179. _Id._
that it has taken against foreign spies found to be operating in the United States.

In a 1999 case tried by the District Counsel in Miami for the now abolished Immigration and Naturalization Service ("INS"), the government made use of a 1958 law that had long been forgotten and apparently never-before used as an enforcement strategy. The government made use of a 1958 law that had long been forgotten and apparently never-before used as an enforcement strategy. When the case of In re Jorge Rodriguez was first tried in the Immigration Court, the assigned Immigration Judge found that the government had "failed to meet its burden of proving the respondent's deportability on the charges against him." The respondent, a known Cuban Intelligence Service ("CUBIS") agent, was being charged with deportability for violating the Immigration and Nationality Act—specifically 8 U.S.C. § 851. The respondent was an "agent handler" of CUBIS based in New York City, who utilized "dead drops" to obtain instructions from senior officials in Cuba and to further relay those messages to other CUBIS agents primarily working in South Florida. The respondent would then receive the intelligence the other CUBIS agents had obtained by clandestine meetings with them primarily in Dade County, Florida and relay it back to the senior officials by use of the dead drops or "burst" radio transmissions upon his return to New York.

The Immigration Judge held that the government had not proved that the respondent had engaged in "espionage" and for that reason determined that the government had failed to meet its burden of proving that Rodriguez had violated the immigration statute by clear, unequivocal, and convincing evidence. As a result, the judge terminated the proceedings.

Daniel N. Vara, Jr., the former Chief Legal Officer for INS and Chief Counsel for Immigration and Customs Enforcement ("ICE") for the Department of Homeland Security ("DHS"), developed a legal strategy and represented the United States throughout the litigation of the case. He was authorized to take an appeal and argued that under section 241(a)(4)(A)(iv) of the Immigration and Nationality Act ("INA"), provided a broad basis for the deportation of aliens who violate "any laws relating to espionage."
Vara argued pursuant to the statute that the government was not required
defendant actually engaged in acts of espionage in order to convict him of
the crime alleged. 189 Furthermore, Mr. Vara argued that the phrase “any law
relating to espionage” encompassed a wide range of statutes, to include 50
U.S.C. § 851, and that failure of Rodriguez to register as a person with
training and knowledge of the espionage tactics of a foreign government in
and of itself made him subject to deportation. 190

Under section 241(a)(4)(A)(i) of the Immigration and Nationality act,
“any alien who has engaged, is engaged, or at any time after entry engages in . . . any activity to violate any law of the United States relating to espionage
or sabotage is deportable.” 191 As noted, 50 U.S.C. § 851 requires registration
of persons who enter the United States who have foreign espionage
knowledge or training and is thus arguably a law “relating to espionage.”

The Board of Appeals agreed with the government that nowhere in this
act did it require the respondent being charged with deportability to have
been convicted of espionage. 192 The Board held that this act only required
an engagement, either in the past or present, in activities related to espionage
for a respondent to be in violation. 193

The Board of Immigration Appeals, in a precedent decision; therefore,
ultimately reversed the lower Immigration Judge’s ruling, and the United
States was able to deport Rodriguez because it proved that he had both
training and knowledge of the espionage tactics of the Cuban government
and had failed to register as required. 194

Since Rodriguez, the government has made frequent use of immigration
law in order to deport suspected spies and has used the registration act theory
as a model for its criminal prosecutions of foreign espionage agents. 195

This law is very useful in that it does not require the prosecution to prove
that a defendant actually engaged in “espionage,” a precise term of art under
the law, and requires only a showing that the person engaged in specific
activities on behalf of a foreign power without having registered as an agent
of that country. This greatly minimizes the government’s obligation to
release highly sensitive information in order to proceed in such criminal
actions. Moreover, when the government specifically proceeds pursuant to the
Immigration and Nationality Act, Classified Information Procedures Act
(“CIPA”) issues do not arise and because such actions are not criminal in

189. Id. at 755.
190. Id. at 755.
192. Id.
193. Id.
194. Id.
195. Id.
nature and involve a different statutory scheme, the government's evidentiary burden is reduced. 196

Prosecuting those alleged to be involved in espionage against the United States can prove to be difficult. With the prosecution of alleged spies comes the struggle between the government's interest in keeping classified information safeguarded and the defendant's constitutional rights at trial. 197 These situations can lead to what the government calls "graymail," which is when a defendant seeks to introduce classified information in court in order to force the prosecution to drop the charges. 198

As this practice became more concerning, Congress enacted the Classified Information Procedures Act ("CIPA") to create uniform procedures for dealing with prosecutions in which classified information is involved. 199 CIPA allows trial judges to rule on the admissibility of classified information seeking to be used in trial in a protected setting. 200 CIPA permits courts to issue protective orders that limit the disclosure of discovery materials to only particular members of the defense team that have been granted special security clearances and cleared, with restrictions, to view and handle such information. 201 Further, CIPA allows for substitutes or redactions of the classified information to be used in criminal courts so long as it does not violate the constitutional rights of the defendant. 202

VII. COMPARISON OF HOW SPIES ARE PROSECUTED IN THE UNITED STATES AND RUSSIA

With instances of espionage clearly being a continuing problem in both Russia and the United States, both countries face barriers when it comes to spies suspected of espionage. Of course, and as noted, with given the two countries' histories in regards to espionage both have a number of laws pertaining to spies, espionage, and counter-intelligence.

In both Russia and the United States, the laws of sovereignty allow the host country to determine the conditions of both admission and continued stay for aliens. Diplomatic relations allow a country to expel diplomats who are determined to be in violation of the rules of their host country.

198. Id. at 4
199. Id. at 2
200. Id.
201. Id.
202. Lee & Garvey, supra note 197.
Diplomatic immunity is a concept created under international law that prevents foreign officials from being subject to courts or other local authorities within that jurisdiction. This immunity extends in part to both their official and personal activities. Compliance with the conditions of their diplomatic status is a requirement and to violate would result in expulsion.

Both the United States and Russia have many laws related to espionage that range in both their requirements and the severity of their punishment. Depending on the country and violation, a person convicted of espionage could be imprisoned anywhere from two years to life or, in some cases, even receive the death penalty.

Additionally, both countries have very complex and sophisticated agencies that are in charge of intelligence and espionage related activities. In each country, there are multiple agencies that have the authority and responsibility to conduct intelligence and counter-intelligence related activities and to ensure that each of their respective governments are not infiltrated by the spies of another.

Both the United States and Russia, as well as most other sovereign nations, engage in espionage. It is clear from the three recent cases discussed earlier in this paper that both countries engage in these tactics and that both have trained spies and are ready and willing to send overseas in order to gain intelligence.

However, unlike the United States, the Russians are not known to use immigration laws to deal with and remove suspected espionage agents. This may be because they do not have to resort to such creative approaches since, in Russia, "due process" is not the same as is afforded in the United States.

VIII. LEGAL ANALYSIS OF LAWS RELATING TO ESPIONAGE IN THE UNITED STATES AND RUSSIA

Diplomatic immunity is an international concept. While the United States receives the benefits of this law, as in the example of Ryan Fogle, this law, at times, allows for those in violation of American law to not be subject to the same degree of punishment.

Before In re Jorge Rodriguez, in order to deal with a foreign espionage agent operating in America in our criminal justice system, the United States had to release a lot more information than they were willing to. Now, however, use of 50 U.C.S. § 851 and similar registration statutes allows the government to make use of immigration law to deport rather than criminally.
prosecute, and/or to criminally prosecute spies without having to actually prove that they engaged in espionage in the United States.\footnote{206}

While it appears obvious that the United States has a very sophisticated intelligence system, one should not be quick to overlook Russia's intelligence model. The Russian intelligence model is one that combines espionage with politics, information warfare, firepower, and economic force similar to that of the United States.\footnote{207} These are all skills that the Russians continued from the days of the Soviet Union and further refined throughout the years.\footnote{208} In fact, "nonmilitary means," such as intelligence work, has become so crucial to Russia that General Valery Gerasimov, head of the Russian army, stated that these means, at times, exceed even those of traditional firepower in their importance.\footnote{209}

Moreover, in the 1920s and 1930s the Soviets created a distinctive method of conducting espionage that allowed them to become very skilled in placing spies in key government positions.\footnote{210} This model had four distinctive phases:

1. to identify candidates, who were often young men and women who were nationals of the country Soviet Russia hoped to gain intelligence on,\footnote{211} (2) to evaluate and recruit the candidates,\footnote{212} (3) to place them in particular organizations and manage their advancement and (4) to exploit them.\footnote{213}

"The longer the third phase took, the more effective the fourth phase would be."\footnote{214}

Another reason why the Russian model of espionage is so advanced is because Russia's president, Vladimir Putin, was a member of the KGB for sixteen years as an intelligence officer.\footnote{215} His knowledge about intelligence warfare, through his experience in the KGB, has presumably allowed for and
contributed to Russia emphasizing and continuing to be both skilled and successful in the art of espionage. 214

Though America is renowned for its work in intelligence, concerns have been expressed with the manner in which this country deals with the subject of espionage. 215 At first glance it may appear as if there are endless loopholes in the laws surrounding espionage in the United States.

From limited incarceration, to skipping criminal action altogether, and opting instead for deportation, expulsion as a persona non grata, or spy swaps, is perceived that espionage is not dealt with as severely as it should be. 216

Those in the government who are actually involved in these cases believe these alternative methods serve their purpose efficiently, effectively and with minimal risks to other national security interests in that they allow such spies to be shut down and rendered useless as espionage agents. 217

Moreover, general perceptions and concerns about damage control are arguable and for the same reason, overstated.

By the time an alleged spy has been arrested, the information that they have obtained has been sent or deleted. 218 Spies are not sent on missions with instructions to gather intelligence and relay that information to their home government “eventually.” Spies are sent on missions to obtain intelligence and relay that information on a real time basis.

Beyond that, prosecuting an alleged spy comes with a price that, at times, the government is not willing to pay. Prosecuting a spy means years of court filings, delays, and taxpayer dollars. Most of all it means potentially having to release classified information that the government needs or wants to remain classified.

Spying, as noted, is also an activity that most countries participate in. Absent situations where acts of violence are associated with espionage activity, there is little to no real incentive for a government to incarcerate a spy, a patriot for his country, for doing the very thing the nation would be guilty of themselves.

Thus, criminal prosecutions should remain the exception and reserved for the most egregious espionage activities, such as where, as noted, a foreign agent happens to commit an act of violence.

214. Id.
215. Martinez, supra note 73.
216. Sheridan & Markon, supra note 58.
217. See generally Sheridan & Markon, supra note 58 (Once labeled a "spy" and removed from a host country, that person has been outed the international intelligence community. Re-assignment as a covert agent to another host country would be virtually impossible and/or meaningless.).
218. See Metkes et al., supra note 59.
Therefore, deporting or trading spies might not be as ineffectual as it initially appears to be. By deporting or otherwise removing a known or suspected spy back to their country in lieu of criminal prosecution, it immediately stops the espionage activity, removes the threat to the host nation, and ultimately, with rare exception, renders that spy useless for future covert intelligence work.219

Most countries engage in espionage, and they realize that there are limitations that accompany what they can do about such intelligence gathering activities against their own nation without chaotic impact to their own spy efforts. That is probably why absent some general considerations, acts of espionage are often not the subject of forceful and continued condemnation by any country.

Dealing with espionage is a careful balancing of national security considerations. A country must engage in counter-espionage to identify espionage, must decide when a known spy’s activities have crossed the line and are no longer tolerable, and must then deal with the spy and his or her activity in a strategic manner and take the course of action that will be most effective in curing the issue within the limitations of its own laws and the knowledge that whatever they do may result in reciprocal action by the affected country.

IX. CONCLUSION

This article has addressed the history of espionage between the United States and Russia, has sought to set forth a presentation and analysis of some of the major misperceptions and fallacies that some may have in regards to how the noted countries deal with foreign intelligence activities, and has provided examples of three recent cases that prove espionage still is just as prevalent today as it ever was. Insight was provided on the background of Russia’s intelligence apparatus and some of the most often used laws relating to espionage in that country were highlighted. This article then gave insight into both the branches of government and laws pertaining to espionage in the United States. Lastly, this article concluded with an opinion on how each country deals with the subject of espionage as affected by its legal limitations, national interests, and the totality of considerations applicable to the subject matter.

Espionage by and against sovereign nations is still pervasive and will always likely be. The laws surrounding these issues, as they relate to the United States and Russia, the subject countries of this paper, are, of course, not perfect and may never be, but they appear to be the most effective and efficient manner available to ensure that the time, money, and efforts

219. See generally Shvetz & Mathews, supra note 58.
employed to combat foreign intelligence activities by a host country are put to good use, and that known or suspected spies are kept in check or prevented altogether from adversely affecting a country’s national security interests.