The Russian Interference in the 2016 U.S. Presidential Election: Analyzing Legal Aspects of Cyber Espionage in International Law

POL 305 – Public International Law: Research Paper

By Alyazya Alkhazraji and Yuvika Bhatia

The context, activities, and area of espionage are extensive. It can be conducted either through hiring spies, people that secretly gather information from within a country or organization, or through an impermissible entry or hacking of technological infrastructures of a country or organization i.e. cyber-espionage. Considering the current context and reality of the global order in the digital age, cyber espionage constitutes a serious threat to established institutions, functioning, and operations of states. In particular, cyber-governmental espionage has become the center of many debates in the current age due to the complicated and extensive area of activities that constitute cyber-espionage. In terms of addressing the issue of cyber-espionage, international law seems likely to be the only institution with jurisdiction to define and govern cyber-espionage as it involves more than two states, with one committing to threaten the security of one or more states. All over the news recently is the recent 2016 U.S. Presidential Election and the Russian interference and has been considered by politicians, government officials, and lawyers as an act of espionage and foreign intervention that had severely undermined the democratic system of the United States. Since espionage is often an extraterritorial state action that transcends across more than two states, this paper aims to assess the legality or illegality of espionage within the framework of international law by putting a primary focus on analyzing the legal or illegal aspects of the Russian Interference in the 2016 U.S. Presidential Election.

Definition of Espionage and Evidence of its Prohibition in Sources of International Law

The Oxford Dictionary defines cyber espionage as “[T]he use of computer networks to gain illicit access to confidential information, typically that held by a government or another organization.”[1] In international law, the definition of espionage has evolved since Article 29 of the 1907 Hague regulations. Today, espionage includes political, economic, environmental, diplomatic, and governmental espionage, etc. alongside military espionage. The legality of espionage in international law with regards to international human rights law, customs, general principles of law, and multilateral treaties have long been debated.[2] Accordingly, the first section of this paper will assess the definition of espionage in international law by looking at scholarly literature on views regarding the legality of espionage within the field of international law along with analyzing evidence available on the prohibition of espionage in customary international law and general principles of international law, two authoritative sources of public international law as stated in Article 38 (1)(b) of the Statute of the International Court of Justice.

1.1. Scholarly literature on the prohibition of espionage in international law

1. John Radsan believes that most developed countries gather foreign intelligence, i.e. sensitive information of other states, either “through consolidated service or a separate foreign service”[3] and they do so because they believe it to be irresponsible not to when looking at it from the perspective of their own state’s interests. The intelligence gathering can comprise of information about political, military, and economic developments of other states because it is of a paramount need to not lose their edge in a faster and digitally integrated world.[4] Loyalties lie towards national interests rather than international ones so until regional and international integration is formed, intelligence services will continue to do their states’ biddings. [5] Each nation shares common principles of espionage because each one is attempting to gain access to secrets of other states, particularly their enemies or those considered a threat. [6] There are no restrictions in the community or market for intelligence on who can be spied on as friendly states also commit acts of espionage against each other. [7] However, the world’s intelligence community is most affected by laws of other states and any international law or convention regulating intelligence-gathering activities. [8]

Similar to Radsan’s view, Catherine Lotrionte states that espionage began as a systematic and publicly recognized state activity, often viewed as essential to the conduct of international relations due to every state consistently conducting espionage. [9] Since the Cold War, states reserved the right to enforce guidelines or statutes for domestic espionage but remained candid about conducting intelligence-gathering activities on foreign states for a period. Later, they started to publicly acknowledge conducting intelligence collection activities by identifying intelligence officials in public. [10] Bear in mind though that despite being significant indicators of state perspectives, such practices must not be interpreted as tolerated penetrations of another state’s territorial integrity. However, the new perspectives can indicate the legality of

intelligence collection if done so within accepted normative parameters. Logically, in the matters of particular acts of spying, the sponsor state's motivation is crucial in determining its lawfulness. If the information pursued were purely contributing to defensive national policies rather than offensive ones, that act would be viewed as claiming greater legitimacy under international law.[11] n the light of ongoing consistent state practice of cyber espionage, it indicates legality, however, the acceptance of intelligence gathering for global security is a radical step away from traditional legal doctrines of within international law.

If we wish to assess the history of espionage in international law, a distinction arises between wartime and peacetime espionage. Most literature addresses wartime espionage committed by people and in which laws of war apply. The rules of espionage during the war are straightforward, considering the Hague Regulations of 1907, the Geneva Conventions, the Protocol Additional to the Geneva Conventions, and other sources.[12] A person in military uniform or one that designates himself or herself as a combatant risks arrest behind enemy lines and if caught, this person is seen as a war prisoner due to the non-deceitful and non-treacherous nature of his scouting or mission.[13] A spy, one without military uniform or designation, is not entitled to war prisoner protections as his deceit leads to severe punishment by captors.[14] However, cyber-espionage most often than not falls under peacetime espionage and does not involve the use of people to gain access to sensitive information but rather through impermissible entries in technological institutions or infrastructure to gather intelligence. Existing literature on peacetime espionage splits the activity into three groups: peacetime espionage is legal or not illegal under international law; peacetime espionage is illegal under international law, and peacetime espionage is neither legal nor illegal.[15]

Geoffrey Dearnest's arguments are a good example of a view that regards espionage is legal and not illegal. He states that attention to peacetime espionage in terms of its legality has lagged behind other developments of international norms concerning intelligence gathering, which is considered to be cyber-espionage. However, despite viewing espionage as an unfriendly act, he does not believe it to be a violation of international law and shows a favorable view to the act. He states that intelligence gatherers, other than actual spies, should not be considered ones if they collect information within the scope of their identities or professions, and said his primary concern is the prevention of hasty labeling of spies. Although, Demarest has not addressed the exploitation of such exclusions of the "spy label," a high probability remains of the exclusions being used as a form of cover or protection to their intelligence officers. Conversely, he argues that spies accused of wartime espionage as opposed to those accused of peacetime espionage should receive a death penalty. Similar to Dearnest's views, Roger Scott states that espionage is not prohibited as "a fundamentally wrongful activity" in international law but the use of the adverb "fundamentally" raises doubts on whether the act should even be considered wrong in any way, shape, or form.[16] Scott defends acts of espionage by providing the argument that it does not violate the jus cogens principle whilst providing the legal support of associating it with the "right of anticipatory or preemptory" self-defense under the UN Charter and international law."[17] Despite an unsteady foundation for peacetime espionage, Scott asserts that covert collection of intelligence in the territory of a state that presents clear threats, through "their past behavior, capabilities, and

expressions of intent,"[18] can be justified as practice protected by the position of the right to self-defense.

On the other hand, Manuel Garcia-Mora believes that peacetime espionage is the international equivalent of delinquency and a total violation of international law.[19] Similarly, Quincy Wright sees peacetime espionage as a violation of a state's duty in respecting the "territorial integrity and political independence of other states."[20] Ingrid Delupuis offers an interesting view concerning the legality of espionage where she states peacetime espionage is illegal under international law if a foreign state's agent is sent into another state's territory.[21] This raises questions on her definition based on the nature of the clandestine activity and it thereby points out two probable definitions: one comprising of intelligence officers entering a country under a false pretense of being diplomats and the second is the limitation of the definition to those sneaking into the state without the awareness of local authorities. .[22] However, Delupis does not qualify espionage as an international crime by providing a fine distinction between "behavior that is contrary to international norms and behavior that constitutes a crime" such as genocide, torture, or other war crimes that can be prosecuted before an international tribunal or court.[23]

Former CIA officials Daniel Silver and Frederick Hitz see the legality of espionage under international law as "oxymoronic." They hold the view that espionage should neither be condoned nor condemned under international law as countries are less accepting of being spied on as compared to when they spy on states, allies and foes alike. Regardless of the clear legality or illegality status of espionage in international law, the officials remain realistic that states commit to spying on other states for matters of self-defense and to satisfy their own interests.[24] This explains the lack thereof treaties and conventions or any other sources of law that specifically prohibit espionage. Christopher Baker (2004) shares the same principle that international law preserves espionage "as a tool by which to facilitate international cooperation," instead of endorsing or prohibiting the practice altogether (p. 1091-1092).[25] Adding to his argument, it does not suffice for states to accept and rely purely on the information provided by other treaty partners without espionage as opposed to intelligence gathering or sharing, as seen in the case of the talks between the Americans and Soviets "over the size of their nuclear stockpiles" during the Cold War.[26]

As a side and unique view, Simon Chesterman sees several functional benefits to espionage for the international community of states and he advises that sharing intelligence "with multilateral organizations could lead the international community to develop new international norms."[27] He states that shared intelligence benefits cases of preemptive military action, justifies targeted financial sanctions against particular actors, and supports international criminal prosecutions.[28] His one-off deal examples show that state cooperation in intelligence sharing will occur only if it serves the state's interests because these examples are slow and indirect methods to infer from and thereby fails to help the legal scholarship to achieve international consensus on the legality of espionage.[29]

At the moment, only special regimes or institutions, like the laws of war, address intelligence explicitly. Legal institutions remain silent on how to deal with diplomatic protection and arms control in terms of intelligence.[30] Additionally, the definition of intelligence is also crucial to that of espionage as it can be either acts committed by spies or covert agents or “territorially intrusive surveillance” that can be classified as an armed attack with the target state being granted the right to self-defense as preserved in Article 51 of the UN Charter.[31] The cases of covert actions that damage property or harm nationals of another country will fall under state responsibility. On the other hand, intelligence gathering and analysis is problematic as it relies on open-source information. [32]

Peacetime intelligence collection has been ignored in international law except with regards to the laws of war. Currently, no rules or a body of rules in public international law deal with the fundamental legality or illegality of espionage but this is disconcerting and remarkable considering the prominent role and practice of espionage in the decision-making process of international relations and political operations.[33] This lack has contributed to the view that espionage is extra-legal as seen in state practice or *opinio juris* of how states deny committing any acts of espionage but they do not conceal it. This consistent practice has given an appearance as a lawful activity that is recognized and this thereby making it serve as custom, an authoritative source of law but since the act is performed in ubiquity, an obscurity is commonplace that makes it difficult to conduct a scholarly inquiry into cyber-espionage.[34] Cyber espionage activities with the same objectives as traditional peacetime espionage would be acceptable state practice under international law if the activities remain within acceptable bounds and limits. These limits must be equivalent to the rules of traditional peacetime espionage to be accepted by other states and within international law.[35]

On a fundamental level, international law is based on the principle of reciprocity due to long-term state practice. States enter into agreements with the promise of honoring their obligations, even those that require restraint in certain ways, to gain reciprocal benefits for each side. According to Lotrionte, espionage or the gathering of secret information offer reciprocal benefits as each side seeks intelligence gathering to understand a foreign state’s capabilities and intentions, information that is of nature not to usually be disclosed freely.[36] As mentioned earlier, if states remain within agreed parameters of acceptable espionage activities, the activities will be allowed to continue by states without holding any liability if they are caught and since each state would like to know what the other is hiding, it clearly shows a common interest shared by each state.[37] Overall, intelligence collection supports the principle of reciprocity in international law through the provision of information shared by one state with others; every state can enjoy benefits from the sharing. The process can facilitate international cooperation through the solidification of state commitments to each other towards a peaceful achievement of mutually shared interests by the gaining of necessary data to make informed decisions and the building of trust between each state.

1.2. Prohibition of espionage in customary international law

Customary law is a crucial formal source of public international law, “which gives to the content of rules of international law their character as law[38].” This type of law is a highly authoritative source of international law because it has been determined to fall under the jurisdiction of the International Court of Justice, according to Article 38 (b) of the Statute of the International Court of Justice. In the Statute, the international custom is accepted based on evidence of widespread and general practice that prohibits certain actions. It is a practice that is accepted as law by and between nations. The source of law is regarded as valid for interpretation and implementation for other international and regional tribunals and courts. [39]

Currently, there is an absence of a right to conduct espionage for states; however, there is a widespread inconsistent practice of state espionage on foreign states. For example, Wikileaks’ release of espionage acts conducted by the United States on Germany and Brazil were not defended by the United States itself. Making matters even more complicated is the mere and consistent practices that deny spies basic rights allowed to war prisoners as well as a possibility of a death penalty sentence. Additionally, customary humanitarian law with regards to armed conflict provides no evidence of state *opinio juris* that gives the right to conduct espionage to states either. Overall, manuals on the laws of war by Israel, the Netherlands, and Belgium do outright state that international law does not prohibit espionage but they do not claim that spying is permissible either by any source of international law, especially with the no evidence of *opinio juris* on the right being generally accepted in state practice. Adding to this lack of evidence that permits espionage, determining state practice of espionage is impossible considering the clandestine nature of the act. The mere existence of intelligence agencies does not constitute state practice of espionage against foreign states because these agencies could be conducting other types of intelligence gathering, analysis, or other acts such as counterespionage, signals intelligence, and domestic espionage. Since releases of acts of espionage only pertain to major world powers rather than other states does showcase an absence of state practice and o*pinio juris* permitting espionage. This does not make customary international law a binding source providing a right to commit espionage but it should not be seen as illegal either.

Many scholars argue that espionage might be legal as a matter of customary international law due to long-standing practice by most states.[40] This argument is based on the principle of custom that supports the existence of an international rule-based on the evidence of a “general practice accepted as law” in many states. Stated in Article 38.1(b) of the Statute as well as implemented through decisions of the CJ, these rules require generally extensive and consistent state practice and *opinio juris,* following the state’s belief that the behavior is required or permitted under international law.[41] However, other scholars believe this argument is flawed due to prior situations of sending states neither acknowledge they sent a spy nor intervene when their spies get captured.[42] Most outright deny having knowledge of a spy’s activities or resolve the issue with the least amount of public attention. This practice shows that espionage must be illegal because of lack of or secret intervention by the sending state to its spy’s defense that they believe is legally wrong.[43]

Based on this reasoning if espionage was legal, states would acknowledge their conduct and behavior, as they would believe their actions are legitimate under international law. An international legal principle of custom is that a rule of law based on state practice is established through a sense of right or legal authority rather than that of wrongdoing or illegality in that state's behavior. However, this view can be seen as naïve considering the delicate complexities of international relations since not acknowledging a spy could prevent a very tense diplomatic discussion rather than a violation of international law based on a sense that that action was considered illegal.[44] Overall, *opinio juris* seems to exist on the practice of espionage primarily due to the mere fact that spies are sent to collect information of foreign states along with domestic legislation that provides legal authority for such information collection activities. This can also apply to cyber-espionage that primarily involves intelligence-gathering activities through technology.

On the other hand, a distinction must be made between customary international law and general principles of international law, another source of law that can govern acts of espionage. [45] In the circumstances of when evidence and criteria are insufficient or not present for customary law, and hence, the International Court may have to recourse to general principles of international law and internal law. [46] This distinction is vital, as several states and international institutions prohibit cyber-espionage because it is the unlawful and impermissible obtainment of sensitive information at a disadvantage of the victimized state.

1.3. Prohibition of espionage by general principles of international law

General principles of international law are recognized sources of binding international law and have been firmly affirmed in Article 38 (1) (c) of the Statute of the International Court of Justice (Pellet, 2012, p. 832).[47] This source of law has been relied upon in several cases and judgments in multiple arbitrations of the ICJ. The rulings from the UK vs. Albania case over the Corfu Channel and the Belgium vs. Spain case over the Barcelona Traction at the ICJ are the best examples. General principles of international law are based on laws from domestic legal systems of every civilized state and they underlie principles and not the law itself.[48] These principles primarily avoid non-liquet situations in judging cases but the Statute does not confine the use of this source of law to this purpose only.[49] Identification of general principles of international law is conducted either through mere assertion or through comparative studies of laws of different states[50] and a good example of comparative studies would be Portugal’s memorial in the ICJ case of Right of Passage Over Indian Territory.[51] These comparative analyses must include a diverse and extensive set of states practicing the same principle of law in their legal systems and traditions, which accordingly provides inference on the general practice of the same principle of law and should be considered at an international level.

With the same principle, conducting a comparative analysis of national legal penal codes of several states will provide us an inference into whether the prohibition of espionage can be regarded as a general principle of law. Twelve states with distinct and diverse legal traditions and heritage prohibit espionage in roughly similar terms. The domestic laws view espionage as the passing of sensitive information about the state by a national or foreign national to a foreign state or agent, with the aim of harming the victimized state's security.[52] This study provides a reasonable inference based on evidence that a general principle of international law exists that forbids espionage conducted by a person, regardless of his or her nationality, on a state's territory. However, in the legal definition of espionage in these national penal codes, the term is defined as the passing of sensitive information to a foreign state only through the means of a living person.

According to Lotrionte (2015), the suggestion of the illegality of intelligence collection under international law is most often than not based on the reasoning that espionage is a criminal activity in many domestic legal systems across different states.[53] It brings in the sense that states do view such activities as unlawful under international law based on general practice. This view is based on the assumption that "[u]nder international law if something were truly legal (or at least not illegal), no state should prosecute those who do it."[54] However, this would clearly lead to misinterpretation of the basic concepts of principles of law recognized by states as an authoritative source of international law. General principles of law maintain supremacy and are based on domestic legal principles of law commonly practiced in all domestic legal systems that it reaches the level of international law as governed by inter-state relations. But international law does regulate the measures and methods used in intelligence collections as well as imposing limitations on the act of collections in specific circumstances.[55] Clearly, these restrictions must not support arguments about either legality or illegality of peacetime espionage because the criminalization of such methods is somewhat different from intelligence collection because they are considered unlawful in international law.

1.4. Overall and additional assessment of the legality of the acts and activities of espionage in international law

What has been established is that espionage is an act of offense when it targets the integrity and security of the state. This is primarily in cases when the act is directed towards harming the government. [56] When determining the legality of espionage, the circumstances and motivation of the states practicing espionage must be considered and analyzed in order to identify their political purposes. Once their motivations are established as causing harm to the other state, espionage becomes a political offense. Article 3 of the 1957 European Convention on Extradition specifies two kinds of offenses: the *délit complexe,* where the act is directed at the political order and private rights; and the *délit connexe,* where the act is closely connected with another act that's directed at the political order and private rights.[57] The challenges that arise in detecting whether espionage is unlawful or prohibited under international law are due to the presence of ambiguity in the main terminologies concerning the specified cases.

This causes a divide in scholarship and views of international lawyers and academic scholars when it comes to the interpretation of the law and thus creates loopholes to justify the states' use of espionage.

As detailed in the previous section, given that cyber-espionage is fairly new to the international law scene, there are no laws that directly and specifically prohibit it. In the case mentioned below, espionage is a form of interference and arguably, it is prohibited by Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights (UDHR). Regardless, espionage is a widespread and generally accepted practice of most civilized nations, which creates a challenge in suggesting that it is prohibited under international law due to general practice in a sufficient amount of domestic and international legal systems or institutions. In addition, the goal of international law is to maintain peace and security and thus creates a loophole that legalizes espionage. For instance, Article 42 of the United Nations Charter permits the Security Council to obtain information in order to maintain international peace.[58]

The Russian Interference of the 2016 U.S. Presidential Elections

The Russian cyber-hacking of the 2016 U.S. Presidential Elections illustrates the difficulties international lawyers and scholars may face in regards to the legality of espionage. It is no question that the hacking should be considered an act of espionage but it's difficult to assess whether it was an illegal intervention. Mainly, this is because espionage is seen as a violation of domestic law rather than international law. Espionage conducted by individuals is unlawful; for instance, in 1942; the U.S. Supreme Court decided that individuals committing espionage are in violation of international law of war.[59] However, international law is quite ambiguous in regards to foreign state interventions, and considering that cyber-espionage goes beyond the state's borders, it becomes even more problematic and vague. Regardless, it is argued that the hacking is in violation of international law in regards to state-sovereignty, self-determination, international human rights law and multilateral treaties.

2.1 The intervention violates Russia's obligations in ICCPR, a multilateral treaty

The hacking breached human rights law with regards to Article 17(1) of the ICCPR – a multilateral treaty signed by 74 states including Russia and the United States – which states the following: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[60] Given that Russia hacked and released e-mails of the Democratic National Committee (DNC), particularly of the Democratic Party candidate Hillary Clinton, their action violated their human rights.[61] Here, the illegality of espionage derives from the use of the terms of "unlawful interference."[62] In addition, Article 17(2) states, "Everyone has the right to the protection of the law against such interference or attacks."[63]

It is not clear whether Russian interference was a threat or not; however, it was an act of interference that was in violation of the treaty. Another point regarding the ICCPR is that some scholars interpret the obligation “to respect” under Article 2, which is often viewed as “too restrictive,” to not be bound by territory.[64] This suggests that Russia must respect the privacy of individuals regardless of their place of residence, which, in this case, it did not. Moreover, the hacking is in violation of the UN Charter’s Article 2(7) regarding foreign intervention, which states that nothing within the Charter authorizes “to intervene in matters which are essentially within the domestic jurisdiction of any state,” would be a better argument, as it is clear on foreign intervention.[65]

Referring back to the ICCPR’s Article 17 regarding the rights of privacy, in the case of cyber-espionage, the term “unlawful” refers to “no interference could take place except in cases envisaged by the law.”[66] That said, the General Assembly also stated that it’s permissible to practice surveillance in order to protect national security against threats including terrorism. Article 17 of the ICCPR, authorizes states to conduct surveillance in order to maintain their security.[67] It is a justifiable and legitimate purpose that may otherwise be regarded as unlawful. This also creates loopholes in laws that may seem clear, which makes outlawing espionage challenging. Furthermore, the concern with international organizations, especially in the case of espionage, is that it is difficult to enforce or guarantee compliance especially with Article 17 of the ICCPR. For example, political surveillance has been common in Argentina since1983. The state continues to breach privacy rights despite domestic and international efforts.[68] However, some scholars argue that Article 17 does not have extraterritorial claims.[69] Meaning, it is bound by territory, thus, Russia is only obligated to respect its own citizens’ privacy. In addition, even the U.S. insists that the ICCPR concerns the government’s conduct towards its citizens and not those that transcend national borders into the global community.[70]

As one can see, ambiguity leads to varying interpretations of treaties and laws, which raises the difficulty of assessing the legality of espionage carried out by states. The differences in domestic and international law also prove to be challenging. Furthermore, espionage is widespread, making it easier to argue that it is not outlawed under international law. In his 1950 dissenting opinion on Namibia, Sir Alrnold McNair argued that the Court is authorized to apply Article 38(1)(c) of the Statute of The International Court of Justice (ICJ), “the general principles of law recognized by civilized nations,” whereby it borrows laws from private institutions and uses them as a guide in international law.[71] Applying this to our case, one can say laws regarding espionage conducted by individuals or individual states as a composite or general practice should be recognized as a general principle of international law or as customary international law. These sources should be used as a guide to defining espionage and discussing its legality. These policies can be sourced from domestic or international laws; e.g. the 1942 U.S. Supreme Court decision branding spying as a breach of the law of war, the prohibition of espionage in Article 17 of the ICCPR, and Article 12 of the UDHR as well as Article 8(2) of the European Court of Human Rights. With the use of Article 38(1) (c), the Russian hacking of U.S. election should be considered entirely unlawful and illegal based on existing scholarship as well as domestic and international practices of the principle of international law that prohibits or illegalizes espionage.

Laws regarding cyber-espionage pose a challenge in international law for multiple reasons. First, domestic laws within high-tech leading states regarding cyber-espionage such as the U.S. are uncertain in nature. Namely, the courts in the United States are not able to able to fully exercise jurisdiction over cyber-related activities including espionage because their traditional legal principles are bound by territory, whereas the internet is a non-physical space consisting of “an interconnected system of networks that connects computers around the world.[72] The use of space in the terminology of “cyber-space” suggests that it can be treated as a place. Regardless, the U.S. Supreme Court’s first opinion on the Internet contains language that hints to the “acceptance of the legal metaphor of cyberspace as a place outside national boundaries.”[73] Being a different type of territory, efforts to integrate cyber-related activities with the traditional principles of law have been faced with controversy.

International law may seem clearer on states conducted espionage on their citizens; however, it also creates loopholes that justify espionage. The United States, Britain, Canada, Australia, and New Zealand were part of a surveillance program whereby they collected and stored mass amounts of data including the location and text messages of their citizens.[74] In the 27th session of the Human Rights Council, the General Assembly discussed and published a report regarding “the right to privacy in the digital age.”[75] In this meeting, the General Assembly announced a consensus resolution to preserve the right of privacy in the digital age, and called states to “respect and protect the right to privacy in digital communication.”[76] The report highly suggests that the practice is unlawful because it violates the right to privacy and should be considered espionage on its own citizens, disrespecting their rights to privacy through sharing sensitive and private information with other states.

2.2. Violation of the notion or principle of domain *réservé* or state sovereignty.

Russian actions are also seen as an attack on state sovereignty in terms of domain réservé: the state’s “exclusive power to regulate its internal affairs without outside interference.” In addition, it is in violation of the 1965 United Nations principle of non-intervention, which reaffirmed the right of every state to chose its own political, economic, social, and cultural structure without foreign interference. The resolution also states: “No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.”[77] The resolution also specifies, “non-physical intervention into a state’s domestic election is also considered to be a violation, not just the use of physical force to sabotage an election within another state,” which further highlights the prohibition of the kind of cyber-espionage conducted by Russia.[78] The hacking is an obvious interference with the U.S. internal affairs that undermines the U.S.’s rights under the UN. Moreover, The Tallinn Manual, an academic source, also supports the notion of domain *réservé* that states that intervention against a state’s political structure is in violation of that principle.[79] The Manual also recognizes that human rights law “may be a constraint on cyber-related activities.”[80]

Russian interference can also be seen as an act against the U.S.'s "sovereign will" because they distorted the electoral results to benefit Trump, who is more sympathetic to Russian interest than Hillary Clinton.[81] The U.S. political system is a democratic government that represents the people's will; as the hacking swayed the results away from the people's will to Russia's will, it is seen as an attack on the U.S.'s sovereignty and on its democratic system. In the absence of their interference, the results may have been different, suggesting that the results do not represent the U.S. sovereign will and that of its people. In terms of satisfying elements such as coercion for it to be seen as an unlawful attack against U.S. sovereignty, some scholars argue that an act does not have to be a "threat" in order to be coercive. Rather, the sine qua non of coercion is that an act encourages change in the state behavior or process, and thus can be applied to the U.S. electoral results.[82]

That said, all these arguments are met with counterarguments; namely, the ambiguity of the terms sovereignty, self-determination, and coercion. International lawyers and scholars view the concept of sovereignty and self-determination differently, which makes it difficult to assess whether Russian actions threatened the U.S.'s sovereignty to begin with.[83] This also applies to the term coercion because some scholars specify that elements of coercion be only met when a state threatens another, causing the threatened state to alter its behavior in order to avoid potential consequences.[84] However, this is not applicable to electoral hacking because we cannot identify whether a threat occurred, or which parties or actors were involved in the threat and that makes the case against espionage particularly weak.[85] Another question that can be raised is whether the self-determination of the U.S. can be threatened as an established state. This is because the concepts of sovereignty and self-determination often concern a state's ability to establish itself. Moreover, The Tallinn Manual, on the explanation of how sovereignty can be violated by foreign interventions, states that "states have not found espionage to be a per se violation of sovereignty, even when those actions take place in and/or have effects in another state."[86] In addition with regards to peacetime cyber-espionage it specifies that the act itself does not violate international law; however, "the method which it is carried out might do so."[87] This problem is seen in other literature that argues against the legality of espionage; for example, Ingrid Delupis argued that espionage is in violation of international law; however, she remains unclear on what is considered "clandestine activity" as mentioned earlier. [88]

In political terms, Ohlin believes the Russian hacking did interfere with U.S. sovereignty, provided the concept relates to the will of the people in terms of electoral results.[89] Democratic government means the government must represent the will of the people and this relates to the relationship called sovereign will. And so in this matter of relation, Russian hacking did constitute a distortion of the sovereign will because it helped elect a candidate sympathetic to the Russian government's interests rather the candidate that represented the desires of the American people. However, international lawyers speak of sovereignty as the right of the state to control its territory, regulate its people and be free from external military aggression and lesser forms of impermissible interventions and interference.[90] So a clear distinction lies in the political definition of sovereignty as compared to its legal definition primarily due to the political one centered on the people and the legal version relates to the state. As stated earlier the Russian interference was against the will of people, a clear mark of association to the political definition. But the closest analog of this definition to international law is the principle of self-determination, which grants the right of every person to determine their political destiny

for themselves, and this particular principle was violated during the election.[91] The Russian interference willed the sovereign will of the Russian people because of their concern on existential threat posed by Clinton's interest in a regime change in Russia,[92] which thereby violated the right of the American people for self-determination.

2.3. The intervention was illegal due to evidence of coercive nature and an illegal usurpation of a government function.

The Tallinn Manual points to a requirement of coercion in order to classify an action as an impermissible intervention. According to Ohlin, the intervention will be seen as illegal if the structure has the following form: "engage in this action; otherwise you will suffer a particular consequence," a coercive threat that will be let go off if it meets the aggressor's demand.[93] The victimized state's compliance to the coercive demand is the most likely alternative to the intolerable consequence the state will have to live with if it does not meet that demand and the key assumption is that the threatened consequence is an illegal or wrongful action.[94] However, if the threatening state has due authority under international law to engage in the threatened consequence, the action primarily is an example of strategic behavior and not coercion. The Nicaragua vs. U.S. judgment, coercion was a doctrinal element flowing through the ICJ's decision and is a good example. The actions of the U.S. constituted an illegal use of force under international law because the U.S. did not have the right to mine the harbor, thereby providing support to the Contras. Due to this reason, the U.S. had conducted an illegal intervention that constituted a use of force in violation of the U.N. Charter and customary international law. [95] The key to a coercive impermissible act is its forceful nature on the target state to meet the threatening state's demand in order to avoid the consequences they would bear from that illegal action.

In terms of applying this principle of coercion to the Russian cyber interference, some would argue the requirement of an actual threat to commit an unlawful act as in the Nicaragua case. The essential ingredient is that the threat pushed the state to behave in a way it would otherwise not do. However, substantial evidence exists to conclude the Russian hacking of the election as illegal coercion.[96] The first would be finding the source of coercion that depends on identifying the individual or group that behaves as the target of coercion. Many would see it be an implied threat to Hillary Clinton so it would prevent her from receiving benefits from the elections and provide a more favorable situation for Russia if Trump was elected in exchange for reciprocal considerations from the Trump administration, similar to the concept of reciprocity mentioned earlier.[97] If Clinton is the object of coercion, the point would be to implicitly inform her to pursue a more conciliatory attitude toward Russia and if she refused to comply, the threatened consequence would be the release of the hacked DNC emails.[98] Perhaps the hacking could also be seen as a threat to more illegal behavior by the Russian government. However, what remains unclear is if this threat was made, either explicitly or implicitly. What would be more beneficial is a holistic approach to determine coercion based on the facts surrounding the intervention rather than searching for theoretical requirements. Scholars conclude that the Russian hacking included coercive elements and thereby rejected an impermissible requirement.[99] Others would argue that a line must be drawn between coercive or corrosive destruction of the proper functioning of the American democracy and they would see the Russian hacking as more corrosive rather counting it as coercive due to the genuine ambiguity surrounding the act. [100]

The cyber hacking was the usurpation of the government function of liberal democracy; in this case, it is the holding of federal-level elections, which is not coercive in nature. The Tallinn Manual includes the conduct of elections as one included in the list of governmental functions, amongst functions such as the delivery of social services and effective diplomatic conduct, that would be affected by the changing or deleting of data. [101] However, despite the fact that the Russian government was accused of releasing private information to the public rather than making changes or omissions, everyone agrees that Russia's tampering with electronic voting counts as a violation of international because counting election votes is pragmatically the U.S. government's function but was usurped by Russian interference.[102] As of now, the evidence does not exist of cyber interference in tampering with the vote-counting process but it does include the disclosure of private information and distribution of fake news stories that violated the right to privacy. In the end, what we are left with is an impression of illegal conduct but no clear doctrinal route towards this conclusion.

Conclusion

The discussed case demonstrates the trouble in trying to assess whether cyber-espionage is legal or not. Some scholars and lawyers make strong cases arguing that espionage is in fact prohibited under international laws; however, cyber-espionage is fairly new in a system that is often limited to territory and individual conduct, and hence, ambiguity in the law creates a surge of debates regarding the issue. Due to common governmental practices of espionage and the controversies surrounding it, there is scope for legal systems to see a shift in regards to espionage wherein the laws regarding when it is lawful and unlawful clear. Applying traditional laws to espionage may be difficult, thus, there needs to be developments in the law that include cyber-related activities that occur in the digital world. Arguably, the Russian hacking sabotaged electoral results, swaying them away from the people's will, which undermines U.S. sovereignty and the democratic system. If it was agreed upon that this was in violation of the law, Russia may have to suffer the consequences of the illegal intervention that threatened the vitality and legitimacy of the U.S. democratic system and its major function for providing the right to self-determination to the will of the American people, as it will be subjected to the jurisdiction of the ICJ through Article 38 (b)(c) under the Statute of the ICJ. The rulings should be from international courts or tribunals that peruse and analyze the violations committed by the Russian government. The ICJ, in particular, does have jurisdiction to the rule over this case through Article 38 (a) by the ICCPR, along with (b) and (c) by customary law and general principles of international law respectively. Their illegal intervention violated personal human rights as proved through the provision of several scholarly views and evidence across the field of international law.