# The International Legal View of Espionage

https://www.e-ir.info/2018/03/30/the-international-legal-view-of-espionage/

VERONIKA PROCHKO, MAR 30 2018

Interpreting international law's approach to a given concept is not without complications, such that even the issues that international law is seemingly explicit about are not without their contested areas. International law in the nuclear and technology era requires constant reinterpretation or reassertion to address new problems, issues, and developments in the international system. One of the issues and developments inexplicit in the United Nations Charter (UN Charter) is espionage. There are various elements to espionage concerning its purpose, methods, and practice, but the important thing to note is that, in the absence of war, espionage is never explicitly addressed in international law (Demarest 1996, 339; Chesterman 2006, 1072). The convergence of international law with peacetime espionage is a highly contested issue, with varying levels of consensus by legal scholars. The arguments for and against the legality of espionage in state practice each have varying interpretations of the UN Charter and other sources of international law, and the following analysis intends to investigate these interpretations and determine the forms of espionage that violate international law, are potentially permissible under international law, or remain virtually unaddressed by international law altogether. Through this investigation, the consensus about what state sovereignty and territorial integrity entail has potentially begun to change since the end of the Cold War, making previous forms of espionage that were not yet considered illegal, such as human intelligence, now illegal, but leaving some new forms of espionage, specifically cyber espionage, almost entirely unaddressed.

The following analysis is comprised of two parts, the first of which defines the two types of espionage: covert operations and covert intelligence, distinguishing between the human and cyber variants of both. The second section discusses the relevant debates concerning the various interpretations of international law surrounding each type of espionage and their legality in the following order: active operations, human intelligence, cyber operations, and cyber intelligence. The international legal concepts of importance to this analysis stem from Article 2(1) and Article 2(4) of the UN Charter (1945): the prohibition of the use of force, the principle of sovereignty and non-intervention, and self-determination, as well as rights stemming from other conventions, such as privacy protection.

"Espionage by definition is intended to occur without detection;" therefore, it is safe to assume that defining and regulating it brings significant complications (Deeks 2015, 314). The forms and aims of espionage differ significantly, especially with the advent of technology; however, espionage can roughly be defined as a "tool for the execution of policy as well as a tool to inform policy" (Scott and Jackson 2004, 4). This definition adequately splits espionage into its two categories: covert operations (a tool for the execution of policy) and intelligence (a tool to inform policy). The first category, covert operations, consists of active operations and cyber operations, which are actions a state takes to influence or affect a foreign sovereign that lack public endorsement by the state and usually remain classified (Fatouros 1976, 193; Jackamo 1992, 992). The forms covert operations take can be divided into three classifications: coercive covert operations, political action, and propaganda (Treverton 1988, 13). The methods of these types of covert operations differ, primarily through the use of active forces and the use of cyber programming, which have an effect on the aim of the forms they take, but ultimately have either a forceful or influential element.

The second category of espionage, covert intelligence, can also be divided into two strands: collection of information and analysis of that information (Radsan 2007, 599; Sulmasy and Yoo 2007, 625). With respect to international law, the initial collection of information is what raises serious and significant legal questions, making it, rather than analysis, of utmost importance as well as highly contested (Sulmasy and Yoo 2007, 625). Intelligence collection itself can be divided into three variants:[1] human intelligence (HUMINT), such as active agents collecting information

through networking and interaction; signals intelligence (SIGINT), such as electronic surveillance or communication interception; and photographic or imagery intelligence (IMINT)[2], such as satellite reconnaissance (Sulmasy and Yoo 2007, 625; Chesterman 2006, 1074; Jackamo 1992, 935). These methods of intelligence collection provide the information states use to guide its decision-making, plan its foreign policy, and predict, influence, or understand the future behavior of its constituents (compare Warner 2009, 9; Chesterman 2006, 1074; McDougal et al. 1973, 365). Therefore, it can be understood that intelligence is an important part of state practice, and the secrecy attached to it, further implies that intelligence is a crucial part to informing state decision-making.

Considering the aim and practical differences between the types of espionage, there are significant aspects to these methods that raise red flags with respect to international law, and it is necessary to analyze the ways in which it is possible for, or can be argued that, espionage can violate international law. The methodical and contextual differences between active operations and human intelligence and their cyber counterparts: cyber operations and cyber intelligence, is paramount when discerning their legality under international law.

To determine the legality of espionage under international law, it is essential first to look at any reference international law makes to the concept. Spying has existed since the beginning of history as a deceptive and risky profession, but in the aftermath of World War II, the international community entered an era devoted to the maintenance of peace, security, and international norms (Radsan 2007, 596). Espionage currently, however, has not been addressed in this new era, thereby remaining only explicitly recognized as an art of war under the law. The law addressing espionage, furthermore, only addresses its prisoner status: spies do not have the same status as scouts during wartime because of the level of deceit accompanying their practice.[3] The Geneva Convention of 1947 and the additional Protocol I added later discuss the treatment of spies upon capture hinging on the circumstances in which they are discovered (Sulmasy and Yoo 2007, 627; Demarest 1996, 332).[4] The discussion of spy treatment during wartime by international law suggests an implied legitimacy to the practice; however, it is still not explicitly declared legal and the application to peacetime espionage is essentially negligible due to the supremacy of state sovereignty. Conclusions about the legality of peacetime espionage, therefore, are difficult to draw from established international law directly, especially since peacetime espionage has a wide range of forms and aims by different states. Such variation requires a distinct interpretation of the law in respect to each varying method and practice of espionage, further discussed in the next section.

As mentioned previously, covert operations each have essentially three possible forms: coercive operations, political action, and propaganda; and, with respect to active operations, the legality of each during peacetime is inherently different than to that of wartime. “The legitimacy of espionage in time of war arises from the absence of any general obligation of belligerents to respect the territory or government of the enemy state, and from the lack of any specific convention against it” (Wright 1962, 12). However, in peacetime, it is evident that international obligations to respect the sovereignty of a state, the self-determination of peoples, and refrainment from the use of force conflict with the main goal of active operations: to either influence or affect a sovereign state. Article 2(4) of the UN Charter explicitly prohibits states from the use or threat of force, which would make operations that use force without authorization by the UN Security Council (Chapter VII) directly in violation of international law.

An example of this can be seen in the use of covert operations by the United States (US) in Nicaragua. Coupled with violations of sovereignty and non-intervention, the International Court of Justice (ICJ) case found the US guilty of using force with charges constituting both direct and indirect action to undermine the Nicaraguan government through deploying American agents, financing Nicaraguan insurgents, and mining waters within Nicaragua’s territorial sea (1986, para. 202-215). The *Nicaragua vs. US* case provides a crucial reassertion of General Assembly Resolution 3314 (1974) which set about providing an expanded definition of aggression to include not only direct forceful action by the offending state, but also any sort of indirect or covert funding, training or supplying of parties known as aggressors to a sovereign state (88).[5] On this basis alone, the first of the categories mentioned in the definition of covert operations, coercive covert operations and related action, in this case, the funding of similar but not directly controlled operations, violate international law, with no qualifications.

However, if a covert active operation lacks this condemning element of use or threat of force or act of aggression, entailing an armed attack or sponsorship of an armed attack, such as the second category of covert operations,

political action, the former violation does not apply. Rather, a different legal issue is raised. Article 2(1) of the UN Charter pledges commitment to "the principle of the sovereign equality of all its Members," which is only further underlined in the ICJ *Nicaragua vs. US* case (1986) declaring the principle of non-intervention and the right of a sovereign state to conduct its affairs as part of customary international law (para. 202). By application, covert operations aimed at influencing or controlling the political affairs of a foreign state by definition violate the principle of non-intervention because this action interferes with a sovereign state's right to control its own internal affairs or function effectively.

Nevertheless, this concept of the law sparks a debate between various international legal scholars, because the extent to which non-intervention applies to unarmed and unaggressive operations is not explicit in the law (Jackamo 1992, 956).[6] Demonstrating the lack of clarity, GA Resolution 2625 addresses the issue of non-intervention as follows:

"No State or Group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic, and cultural elements, are in violation of international law" (1970, 123).

The issue raising debate is the context in which the principle of illegal interference is evoked. The resolution can be argued to be referring to armed attacks only and not to be stretched to include nonaggressive acts; however, the phrase "all other forms of interference" leave the door open to various interpretations by states as to what this means.[7] A handful of legal analysts claim that intervention implies a concept of coercion that is not always present in covert operations that lack behavior which constitute the use of force or an act of aggression, maintaining that the UN Charter only explicitly prohibits *armed* intervention and that stemming from intervention of aggressive nature, as also referred to in GA Resolution 2625 (Jackamo 1992, 959; Ohlin 2017, 1580). This would suggest that states in 1970 were not comfortable extending this definition because that would require potentially limiting themselves in a way that they were not prepared to at the time. Evidence of this can be seen in the U-2 incident in 1960, when a US reconnaissance plane was shot down over the Soviet Union (USSR) while effectively 'spying' on the USSR; yet, this act was not condemned as illegal by the international community and was not seen as an act of aggression under the interpretation of the UN Charter 2(4) and GA Resolution 2625 (Wright 1960, 844; Demarest 1996, 341).

However, ten years later, there appeared to be a change in the consensus of states surrounding the principle of sovereignty with GA Resolution 36/103 (1981). This resolution recalled Resolutions 2625 and 3314 and added the phrase "in any form or for any reason whatsoever" to the principle of non-intervention, going on to expand on what else states believed the right included:

"(a) Sovereignty, political independence, territorial integrity, national unity and security of all States, as well as national identity and cultural heritage of their peoples;

(b) The sovereign and inalienable right of a State freely to determine its own political, economic, cultural and social system, to develop its international relations and to exercise permanent sovereignty over its natural resources, in accordance with the will of its people, without outside intervention, interference, subversion, coercion or threat in any form whatsoever;

(c) The right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations, based, inter alia, on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order" (1981, 73).

This resolution is important to the legal understanding of non-intervention and state sovereignty because although GA Resolutions do not constitute law, they reveal a great deal about *opinio juris* as well as set into motion interstate dialogue concerning how a transformed understanding of certain concepts could be emerging. Differentiating intervention, interference, subversion, coercion and threat as separate entities is crucial to understanding the legality

of unarmed covert operations. The political aim of this type of covert active operations by its nature would constitute a violation of a state's sovereignty under Resolution 36/103's interpretation of Article 2(1) and 2(4) of the UN Charter: interference, intervention, or subversion in "any form" constitute a breach of a state's sovereignty and right to non-intervention.

However, some academics argue that that the legality of covert action itself, then, depends "entirely on its nature" (Forcese 2016, 75) leaving a door open to other forms of active operations to be permissible under international law. The final form of active covert operations characterised by Treverton (1988, 73) is propaganda, which, in theory, does not hinder state function or violate political independence, suggesting its overall permissibility. Nevertheless, by applying the interpretation of GA Resolution 36/103 to the principle of non-intervention, covert propaganda directly violates a state's international right to "develop fully, without interference, their system of information and mass media" especially surrounding issues of politics, economy, and culture. This understanding of the principle of non-intervention "in any form" has serious implications for the legality of this third and final form of active operations since regardless of its method, goal, and aim, propaganda is seemingly recognized by states to constitute a breach of sovereignty protected by Article 2(1) of the UN Charter. It is in this sense, that although there is no codified extension of this definition of sovereignty, states' opinions concerning its scope are beginning to adopt more restrictive discourse.

The second strand of espionage, covert intelligence, has a significant amount of contradictory literature surrounding its legality in international law, but one indisputable attribute of intelligence collection is that it is referenced and governed by domestic law as a criminal prescription (compare Demarest 1996, 330; Sulmasy and Yoo 2007, 627; Chesterman 2006, 1077; McDougal et al. 1973, 394). However, in international law, the issues surrounding the legality of human intelligence alone, discounting cyber intelligence for the time being, are of great legal debate. Radsan(2007, 602) defines three camps concerning the legality of espionage in general, but this section will utilise his observation as follows: those opposed to, those in favour of, and those sceptical to the international legality of human intelligence collection .

Those who argue that human intelligence is illegal return to Article 2(4) of the UN Charter with a focus on the words "territorial integrity". A staunch advocate for this view, Quincy Wright (1962, 12), argues that "any penetration of the territory of a state by agents of another state in violation of the local law, is also a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states". Although predating GA Resolution 36/103, Wright is supporting its interpretation that violations of the territorial integrity and political independence of a state go beyond the use or threat of force and acts associated as defined by the *ICJ Nicaragua vs. USA* case and GA Resolution 3314. Supporting this interpretation, Ingrid Delupis (1984, 67) agrees that human intelligence collection entails a violation of territorial integrity, claiming that it is "illegal under international law in time of peace if it involves the presence of agents sent clandestinely by a foreign power into the territory of another state", which is precisely what human intelligence itself would require. Therefore, according to Wright and Delupis the physical presence of an agent in foreign territory violates the non-intervention principle as interpreted by GA Resolution 36/103.

The second camp, however, finds issues with this overarching claim by Delupis and Wright in that if human intelligence was as fundamentally illegal as they claim, the international community would have explicitly condemned it. The lack of international discussion of human intelligence collection constituting a violation of territorial integrity seems to imply that the act is not severe enough to fall into the offensive categories defined in the UN Charter and GA Resolution 36/103.[8] Other academics see this lack of outcry against human intelligence more as a reluctant admission of lawfulness (McDougal et al. 1973, 394) and others as a foundation for practice (Sulmasy and Yoo 2007, 627; Scott 1999, 217; Smith 2007, 544).[9] However, the argument of mere lack of condemnation constituting practice is relatively weak in terms of the evolution of international law.

Other proponents of human intelligence as permissible under international law recognize the territorial integrity violation of the practice, but claim it is essential for national security and ultimately peace (Sulmasy and Yoo 2007, 637). This argument is much sounder as it develops further into a corollary of the actively evolving norm of peremptory self-defence. Active defendants of this justification for territorial intrusion, Scott and Baker, claim that

human intelligence is an inalienable element to a state's right to self-defence and that the destructiveness of modern nuclear weapons and unpredictability of terrorism make intelligence permissible to support this right (Scott 1999, 224-225; Baker 2004, 1096-1097). An issue with this line of thinking is that peremptory self-defence is reserved only for when an armed attack is imminent and unavoidable through any other means; and, for the accusation to be reliable, the human intelligence required would have to be well-established and thorough, thereby not adhering to the condition of immediate threat and not fulfilling the Carolina case criteria (Wright 1962, 18).

However, preventing a state from determining if there is an immediate threat directly infringes on a state's ability to exercise peremptory self-defence: human intelligence allows states to prepare and protect themselves with foreknowledge about potential threats (Scott 1999, 224; Baker 2004, 1096). Just as with the use of force within the argument of peremptory self-defence, it is up to the state to establish a long-standing threat, intent, and capacity to justify action, that is the active penetration of agents into a foreign state's territory with the intention of breaking its domestic laws to obtain information relevant to the security of the interested state (Scott 1999, 225). Nonetheless, peremptory self-defence itself is still evolving under international law and is a highly contentious issue, so by relation, is this justification for the territorial intrusion of human intelligence collection.

The last camp concerning the legality of human intelligence collection are the sceptics. The academics in this camp argue that human intelligence is neither legal nor illegal according to international law, and do not see espionage ceasing to be practiced by states, a consensus emerging, or an incentive for regulation (Radsan 2007, 623; Ratner 2007, 539). Proponents of this view of espionage do not agree that human intelligence constitutes a serious violation of territorial integrity and, in the absence of explicit law, claim a neutral stance on espionage in general, which effectively invokes the judgement of the 1927 *Lotus Case*. Two applicable rulings and precedents emerged from this case, the first being: "every State remains free to adopt the principles which it regards as best and most suitable" (P.C.I.J. 1927, para. 19) and the second: "it is for those who assert the existence of a rule of law restricting state activity to show such a restrictive rule exists" (Stone 1962, 33). The fact that states tend to deal with offenses of espionage domestically would suggest the application of this principle; and since many states practice forms of espionage themselves, they do not want to contest offenses in the international legal system for fear of losing control over the issue (Bowman 1995, 328). This legal view of human intelligence collection practically dismisses GA Resolution 36/103's relevance to espionage at all, thereby ignoring the shifting position of states concerning territorial integrity which would suggest a significant element missing in the sceptic legal argument. Nonetheless, if not a good legal basis for the legitimacy of human intelligence, as an explanation of state behavior, the application of the Lotus principle remains useful and will be utilized concerning cyber intelligence.

Inexplicit issues in international law are at the core of cyber espionage due to its recent development and rapid capability advancement. This method of espionage draws its own debate about the legality of espionage because it circumvents the main violations of law applicable to the methods of human intelligence and active operations. Firstly, concerning the legality of cyber operations, a slightly altered approach to the categories of active operations is necessary. In the world of cyber operations, the concept of armed attack must be expanded beyond its material sense. According to the Tallinn Manual, any cyber operation that causes damage either in terms of casualties or sabotage amounts to a violation of the target state's sovereignty as well as a cyberattack (Schmitt 2013, 16, 106, 195). This action would, like that demonstrated previously in the case of active operations, constitute a breach of international law under Article 2(4) of the UN Charter prohibiting the use of force or act of aggression.

There are, similar to those of active operations, two other possible forms of cyber operations: influential operations and propaganda. It is important to note the nature, method, and goal of these operations are highly contextual. Nevertheless, Ohlin (2017, 1579-1598) provides a comprehensive breakdown of how influential cyber operations or cyber propaganda can violate two parts of the UN Charter: the political independence of the state and the self-determination of peoples, through the example of the recent interference by the Russian Federation in the US elections in 2016. A violation of a state's political independence constitutes a disruption of governmental function, that is interfering in affairs that are in the sole jurisdiction of the state. If a cyber operation were to interfere in a governmental process, election, or service, this would constitute a breach of international law; however, in the case of Russian interference in the US elections, there is no evidence of tampering with vote-tabulation or other governmental functions, so this is not the case (Ohlin 2017, 1593-1594).[10] But were Russia to have interfered in

the voting process, that would have constituted a breach of international law, as it would have been seen as a breach of political independence under the interpretation of Article 2(4) by the GA Resolution 36/103. Ohlin (2017, 1594-1596) goes on to argue that Russian interference did in fact break international law because it infringed on the American citizens' right to self-determination and choose their own government in accordance with the UN Charter. Despite the legal potential of this argument, evidence and severity of cyber acts like that of propaganda are incredibly difficult to trace, track, and tabulate, thereby making the prospect of this kind of espionage receiving a sound legal condemnation from the international community highly improbable. Nonetheless, cyber operations short of the use of force and tampering with governmental function appear permissible by application of the Lotus principle, mainly due to their lack of attention under current international law.

To determine the legality of cyber intelligence, it is necessary to distinguish between the different kinds of electronic surveillance. Deeks (2015) and Forcese (2011) both discuss the difference between domestic, or territorial, foreign, or extraterritorial, and transnational surveillance[11] and how each raises different international legal concerns.[12] With the concept of extraterritorial surveillance, a debate similar to that of human intelligence arises around the principle of territorial integrity. Forcese (2011, 204-205) concludes that there is still general ambiguity about whether or not it constitutes a breach of the territorial sovereignty of a state despite lacking the kinetic, yet still contentious, aspect of physical presence of intelligence agents. The reasons behind this debate are, rather, the territory in which the information is intercepted or collected is under the sovereign control of a foreign state, so obtaining that information covertly for an external power is a violation of the targeted state's territorial integrity.

This understanding is what prompted the Canadian Security Intelligence Service Act of 2008 (CSIS) which ruled that a warrant authorizing extraterritorial surveillance would "therefore be authorizing activities that are inconsistent with and likely to breach the binding customary principles of territorial sovereign equality and non-intervention, by the comity of nations" (CSIS, para. 52). Although this is a domestic policy applicable only to Canada, such as the US Security Act of 2002 and others before it, it sets out an interpretation of the law for the international community to see, which recognizes the conditions of territorial integrity set out by GA Resolution 36/103 as 'binding customary principles'. Domestic policy is one of the starting points for the development of international customs, thereby making the CSIS Act important in spite of its range. Therefore, just as the argument against human intelligence, under the GA Resolution 36/103's interpretation of Article 2(4) of the UN Charter extraterritorial surveillance without the consent of the targeted state constitutes a breach of international law.

However, this is not the case with transnational surveillance, which intercepts information from outside the target state, thereby circumventing the principle of territorial integrity. But, the second legal debate within cyber intelligence that is applicable to both transnational and extraterritorial surveillance is that of privacy protection. This legal question is raised not because it can prohibit cyber intelligence as a whole, but rather could place constraints on it or frustrate its efforts if considered applicable. The debate surrounds whether Article 17 of the International Covenant on Civic and Political Rights (ICCPR) could be applied to "foreign nationals outside the territory of the state party" (Deeks 2015, 307). If the conditions of privacy rights were to apply to citizens in territory outside the acting state's control, the obtainment of a warrant would compromise the whole covert aspect of cyber intelligence. Combating this, Forceses (2011, 207) maintains that by definition the spying state cannot exercise effective control over the surveilled individual, therefore making the ICCPR privacy protections inapplicable. From this standpoint, it is legally sound to conclude that unless further development in the debated jurisdiction of the ICCPR occur, privacy laws have no bearing on the legality of transnational surveillance leaving it altogether unaddressed by international law.[13]

Overall, through the discussion of the literature on espionage, it appears that international law is in the process of changing to include any form of physical territorial intrusion as a violation of sovereignty. The fact that in 1960 the U-2 incident was never condemned as an act of aggression shows that at the time the concept of territorial integrity was considered only applicable to acts of aggression and the use of force; however, GA Resolution 36/103 now implies that territorial integrity extends to include various forms of intrusion. With the potential of the development of *opinio juris* surrounding this resolution, states seem to be changing their view on what constitutes intervention. Therefore, by application active operations and human intelligence collection without the consent of the target state are essentially illegal under international law with some forms of the former for specific reasons less contentious, like use of force and political independence infringement, and the latter for violation of the expanded conception of territorial

integrity. The only exception to the expansion of the meaning of territorial integrity would be Scott's application of the evolving principle of peremptory self-defence which by application could potentially make the gathering of human intelligence legal in extraordinary cases. However, the stance towards these practices after the end of the Cold War is evolving to be more restrictive and condemning of intervention into a state without its consent by any means.

There is a significant implication surrounding espionage that it operates on a legal-until-caught basis; yet by this assumption, suggestions of legality through practice would ultimately open a whole new debate, especially with the capabilities demonstrated by cyber intelligence and cyber operations that were unforeseen by the UN Charter. Nonetheless, the general practice of espionage cannot be and is not explicitly illegal according to international law, and it is up to states and other international actors to apply and interpret the law to the specific contexts in which covert tactics are used. It is in these circumstances and contexts in which certain covert tactics are practiced that questions of legality emerge. Perhaps the more debatable and unclear element of espionage that international law has left open to interpretation and undeliberated is that of cyber operations that do not use force or infringe on political independence and cyber intelligence that is conducted from outside the target state. Whether states will continue to evolve their conception of what state sovereignty constitutes to extend beyond physical borders to more virtual ownership of information and media and whether that conception expansion is at all feasible in an age of technology are things to consider when predicting the future of international law.

**References**

Baker, C. D. (2004) 'Tolerance of International Espionage: A Functional Approach', *American University of International Law Review,* 19:5, 1091-1113.

Bowman, M. E. (1995) 'Intelligence and international law', *International Journal of Intelligence and Counterintelligence,* 8:3, 321-335.

*Canadian Security Intelligence Service Act (Re)* (2008) F.C. 301.

Chesterman, S. (2006) 'The Spy Who Came in from the Cold War: Intelligence and International Law',*Michigan Journal of International Law,* 27, 1071-1190.

*Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States* GA Res. 36/103, UNGAOR, 36th Sess., Supp. 51, U.N. Doc A/36/761 (1981) 78.

*Declarations on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.* GA Res. 2625, UN GAOR, 25th Sess., Supp. 28, U.N. Doc. A/8082 (1970) 121.

Deeks, A. (2015) 'An International Legal Framework for Surveillance', *Virginia Journal of International Law,* 55:2, 291-368.

*Definition of Aggression* GA Res. 3314 (XXIX), UN GAOR 29th Sess., Supp. 31, U.N. Doc. A/9890 (1974) 88.

Delupis, I. (1984) 'Foreign Warships and Immunity for Espionage', *The American Journal of International Law,* 78:1, 53-75.

Demarest, G. B. (1996) 'Espionage in International law', *Denver Journal of International Law and Policy,* 24, 321-348.

Fatouros, A. A. (1976) 'Covert Intervention and International Law', *American Society of International Law Proceedings,* 69, 192-194.

Forcese, C. (2011) 'Spies Without Borders: International Law and Intelligence Collection', *Journal of National*

*Security Law & Policy,* 5, 179-210.

Forcese, C. (2016) 'Pragmatism and Principle: Intelligence Agencies and International Law', *Virginia Law Review,* 102, 67-84.

Gomaa, M. M. (2004) 'The Definition of the Crime of Aggression and the ICC Jurisdiction over that Crime' in M. Politi and G. Nesi (eds) *The International Criminal Court and the Crime of Aggression* (Hants: Ashgate Publishing Limited), 55-78.

Jackamo, T. J. I. (1992) 'From the Cold War to the New Multilateral Order: The Evolution of Covert Operations and Customary International Law of Non-intervention', *Virginia Journal of International Law,* 32, 929-978.

McDougal, M. S., Lasswell, H. D. and Reisman, W. M. (1973) 'The Intelligence Function and World Public Order', *Faculty Scholarship Series,* 365-448.

*Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)* (1986) I.C.J.14, 181 (June27).

Ohlin, J. D. (2017) 'Did Russian Cyber Interference in the 2016 Election Violate International Law', *Texas Law Review,* 95, 1579-1598.

Radsan, A. J. (2007) 'The Unresolved Equation of Espionage and International Law', *Michigan Journal of International Law,* 28:3, 596-623.

Ratner, S. R. (2007) 'Introduction', *Michigan Journal of International Law,* 28:3, 539-542.

*S.S. Lotus (Fr. v. Turk.)* (1927) P.C.I.J. (ser. A) No. 10 (Sept. 7).

Schmitt, M. N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press).

Scott, L. and Jackson, P. (2004) 'Journeys in Shadows' in L. V. Scott and P. D. Jackson (eds)*Understanding Intelligence in the Twenty-first century* (London: Routledge Taylor & Francis Group), 1-28.

Scott, R. D. (1999) 'Territorially Intrusive Intelligence Collection and International Law', *Air Force Review,* 46, 217-226.

Smith, J. H. (2007) 'Keynote Address', *Michigan Journal of International Law,* 28:3, 543-552.

Stone, J. (1962) 'Legal Problems of Espionage in Conditions of Modern Conflict' in R. J. Stanger (ed)*Essays on Espionage and International Law* (Columbus: Ohio State University Press), 29-43.

Sulmasy, G. and Yoo, J. (2007) 'Counterintuitive: Intelligence Operations and International Law',*Michigan Journal of International Law,* 28:3, 625-638.

Treverton, G. F. (1988) *Covert Action: The C.I.A. and the Limits of American Intervention in the Postwar World* (London: I.B. Tauris & Co Ltd).

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, Available at: http://www.un.org/aboutun/charter [Accessed 1 November 2017].

Warner, M. (2009) 'Wanted: A definition of 'intelligence" in R. Aldrich, C. Andrew and W. Wark (eds)*Secret Intelligence: a Reader* (London: Routledge Taylor & Francis Group), 3-11.

Wright, Q. (1960) 'The Legal Aspects of the U-2 Incident', *The American Journal of International Law,* 54:4, 836-854.

Wright, Q. (1962) 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' in R. J. Stanger (ed)*Essays on Espionage and International Law* (Columbus: Ohio State Unversity Press), 3-28.

**Footnotes**

[1] There is a fourth source of intelligence collection called "open source" intelligence, but it will not be discussed in this essay as it has no dispute with international law.

[2] For this essay, SIGINT will be referred to in greater detail (by the name electronic surveillance or cyber intelligence), since the international law regarding satellite (IMINT) intelligence and space in general have a completely different legal focus under international law that cannot be addressed in this paper.

[3] The treatment of spies is fundamentally an issue of distinction. Historically, treatment of spies was more severe since spies are soldiers posing as civilians, rather than scouts who remain true to their soldier status. (*see* Sulmasy and Yoo 2007, 627-628).

[4] *See* Geneva Convention of 1949, Article 5, at 153 and Protocol Additional to the Geneva Conventions of 12 August 1949, Article 46 at 34-35.

[5] It is important to note that there is no other existing definition of aggression other than the one outlined in General Assembly Resolution 3314 (XXIX) making the expansion of the definition of aggression not explicitly codified in international law but still a rather strong representation of what states consider it should be (*see* Gomaa, 2004: 74).

[6] Jackamo (1992, 956-961) discusses the codification of the duty of non-intervention in multiple bilateral and multilateral treaties since 1933; however, he notes that the precise scope of non-intervention has not been defined, thereby leaving interpretation to the General Assembly and the international judicial system.

[7] For corresponding observations concerning similar clauses in certain treaties, like the OAS Charter, the Helsinki Final Act, and the Pact of League of Arab States, *see* ibd. at 957-960.

[8] For more discussion of the insignificance of intelligence collection as a territorial affront see Bowman (1995) at 223; Ohlin (2017) at 1580; and Jackamo (1992) at 935 and 959.

[9] All these arguments are very similar in logic and evidence only differing in phraseology.

[10] It is important to qualify that these judgements are made based on the information available. The recentness and covert qualities of this incident do, however, postpone any kind of formal and certain decision concerning the facts surrounding the event.

[11] While domestic surveillance is governed by various domestic laws and international humanitarian law, this essay is primarily concerned with the legality of extraterritorial and transnational cyber intelligence.

[12] For a comprehensive breakdown of the legality and forms of cyber intelligence see the diagram in Forcese (2011) at 184 and 209.

[13] Forcese (2011) does, however, mention that there are some kinds of communication and information that transnational and extraterritorial electronic surveillance cannot legally intercept. [e.g. diplomatic communication as prescribed by the Vienna Convention on Diplomatic Relations] (209).

*Written by: Veronika Prochko*

*Written at: The University of St Andrews*
*Written for: Dr Mateja Peter*
*Date written: November 2017*