Articles

"Don't Do as I Do"—The US Response to Russian and Chinese Cyber Espionage and Public International Law

By Patrick C. R. Terry[*]

Abstract

The Russian government is accused of hacking emails circulating among senior members of Hilary Clinton's campaign team to support President Trump's election in 2016. This was not the first time the United States was the target of massive cyber espionage: The Chinese government is believed to have gained sensitive information on 22.1 million US government employees through "cyber intrusions" in 2014. This Article will examine whether cyber espionage of this kind is unlawful under public international law and will conclude that it is. Specifically, such espionage can result in a violation of territorial sovereignty and will likely violate the principle of non-intervention in the internal affairs of other States. Yet, based on the controversial "clean-hands-doctrine," past US actions in the realms of cyber espionage and intervention may well invalidate any claims it asserts against Russia or China.

[*] Patrick C.R. Terry is the Dean of the Faculty of Law at the University of Public Administration in Kehl, Germany. He holds a Ph.D. in public international law, a Master of Laws degree in International Law with International Relations (both University of Kent, U.K.), and two German law degrees.

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

A. Introduction

Following the recent allegations of Russian interference in the electoral process in the United States, the issue of cyber espionage[1] has again gained some traction. The Russian government has been accused of initiating the hacking of emails circulating among the leaders of Clinton's Democrats. These emails were leaked, it is alleged, to embarrass Clinton and her party and thus support Trump's campaign. The US, under former President Obama, reacted to these accusations by expelling Russian diplomats and imposing further sanctions on Russia. Russian behavior in this respect was deemed completely unacceptable.[2]

This was not the first time the US became the target of massive cyber espionage. It is claimed that as early as 2014, the Chinese government had managed to gain sensitive information on 22.1 million US government employees by the way of "cyber intrusions."[3] US officials at the time stated that such actions "cannot go unanswered."[4] This Article will examine whether this kind of cyber espionage through email hacking, which was most likely conducted remotely, without any spy ever having left Russia or China, actually violates public international law.

In public international law, cyber espionage arguably forms the most controversial aspect of activities commonly associated with the term "espionage," as it does not necessarily involve an infringement of another State's sovereignty. In many other cases of espionage—for example, in employing active spies on another State's territory or using embassies and consulates to eavesdrop on foreign governments—obvious violations of territorial sovereignty allow a rapid classification of such activities as unlawful.

---

[1] *See Cyber Definitions*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, https://ccdcoe.org/cyber-definitions.html (providing a definition for "cyber espionage" by country); Ella Shoshan, Applicability of International Law on Cyber Espionage Intrusions 14–15 (2014) (unpublished Ph.D. dissertation, Stockholm University) (on file with author).

[2] *See* OFFICE OF THE DIRECTOR OF NAT'L INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS:" THE ANALYTICAL PROCESS AND CYBER INCIDENT ATTRIBUTION (Jan. 6, 2017), https://www.documentcloud.org/documents/3254229-ICA-2017-01.html#document/p1; Luke Harding, *Top Democrat's Emails Hacked By Russia After Aide Made Typo, Investigation Finds*, THE GUARDIAN (Dec. 14, 2016), https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds; David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, NEW YORK TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?_r=1.

[3] *See* David E. Sanger, *Cyberthreat Posed by China and Iran Confounds Whitehouse*, NEW YORK TIMES (Sept. 15, 2015), https://www.nytimes.com/2015/09/16/world/asia/cyberthreat-posed-by-china-and-iran-confounds-white-house.html; Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, THE WASHINGTON POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.319beab5403b.

[4] *See* Sanger, *supra* note 3.

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

In this Article, I will argue that most cases involving cyber espionage conduct from abroad are contrary to public international law because such conduct: 1) can sometimes result in a violation of territorial sovereignty; 2) often violates the principle of non-intervention in the internal affairs of other States; and 3) can also contravene the principle of sovereign equality.[5] Finally, the Article will conclude that the US was justified in denouncing Russia and China, provided there was sufficient evidence to suggest Russia and China were the originators of the respective hacking.

The irony of these events cannot be overlooked. After all, Snowden's revelations suggest massive US cyber espionage attacks against other countries, which include allies like Germany.[6] The US attitude so far seems to be that such actions are, if not justified under public international law, then certainly not contrary to it.[7] In fact, past US attitudes and actions in the realms of cyber espionage and intervention may invalidate any claims against Russia or China because of the controversial "clean-hands-doctrine." But now that the US itself has become a victim of such actions, the US government's attitude regarding the desirability and legality of cyber espionage may well undergo a welcome process of transformation.

It should be noted that this Article will not examine whether there is sufficient evidence to support the allegations made against Russia or China. The Article will also only deal with cyber espionage initiated by States in peacetime. Furthermore, the question of whether cyber espionage violates international human rights law will not be discussed.

[5] The principle of sovereign equality will not be discussed here, as its application does currently not seem relevant to the allegations made against Russia and China; for more details on this issue, *see* Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), General List No. 156, Order (March 3, 2014), http://www.icj-cij.org/docket/files/156/18078.pdf (focusing especially on para. 27).

[6] James Ball & Nick Hopkins, *GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief*, THE GUARDIAN (Dec. 20, 2013), http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner; Patrick Beuth & Kai Biermann, *Das Spionage-System Prism und Seine Brüder*, DIE ZEIT (June 13, 2013), http://www.zeit.de/digital/datenschutz/2013-06/nsa-prism-faq.

[7] *NSA Skandal: US-Abgeordneter Rechtfertigt Lauschangriffe*, DER SPIEGEL (Oct. 27, 2013), http://www.spiegel.de/politik/ausland/us-abgeordneter-peter-king-rechtfertigt-lauschangriffe-a-930292.html (referring to US Representative Peter King, member of the Homeland Security Committee and Chairman of the Sub-Committee on Counterterrorism and Intelligence); *Warum die USA Schröder und Merkel Abhörten*, BILD ONLINE (Sept. 14, 2014), http://www.bild.de/politik/ausland/nsa/ex-nsa-chef-hayden-warum-die-usa-schroeder-und-merkel-abhoerten-37659540.bild.html (reporting interview with ex-NSA-Chief Hayden).

B. Is Cyber Espionage Contrary to Public International Law?

I. Violation of Territorial Sovereignty

The difficulty in assessing cyber espionage's legality in public international law rests on the seeming lack of violations of territorial sovereignty that are inherent in other classical espionage activities. Spying by government officials abroad, bribing foreign government officials in order to obtain secret information, and using embassies or military bases abroad in order to spy on foreign governments all involve the exercise of executive or governmental power by one State on the territory of another without this other's permission. Such actions violate the victim State's territorial sovereignty and political independence and are thus contrary to international law.

Cyber espionage, in contrast, very often does not involve the physical presence of "a spy" on the target State's territory. Rather, cyber espionage is usually conducted remotely, without the spy ever leaving their home country. This makes it difficult to argue that the victim State's territorial sovereignty has been violated. The European Court of Human Rights (ECHR) in dealing with a similar—though not identical—situation, rejected the claim that such activities necessarily involved the violation of another State's territorial sovereignty:

> Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants have failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.[8]

As far as data stored on servers located in the US is concerned, however, the situation differs from the case decided by the ECHR. The data is not intercepted during transmission at an unknown location outside the US, but at its source within the US. In order to assess the implications of this, it is necessary to examine the meaning of territorial sovereignty. Although the precise definition of sovereignty is very controversial, there is widespread agreement as to its core—territorial sovereignty—which the International Court of Justice (ICJ) has described as "an essential foundation of international relations."[9] Territorial

[8] *See* Weber and Saravia v. Germany, 2006 XI Eur. Ct. H. R. 309, para. 88 (2006); Re Canadian Security Intelligence Service Act, [2009] F.C. 1058 (Can.).

[9] *See* Corfu Channel Case (U.K. v. Alb.), Judgement, 1949 I.C.J. 4, 35 (Apr. 9); *see also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgement, 2005 I.C.J. 168, para. 165 (Dec. 19).

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

sovereignty undoubtedly encompasses a State's "right to exercise therein, to the exclusion of any other State, the functions of a State,"[10] which, of course, means that a State "may not exercise its power in any form in the territory of another [S]tate."[11]

Based on this definition, it could well be argued that the intrusion of Russian and, or Chinese government officials[12] into data stored on servers located on US soil violated the US's territorial sovereignty. Russian or Chinese government agencies were exercising governmental functions on US territory without the US government's permission. That these actions were most likely undertaken remotely—that is, without any Russian or Chinese spy entering US territory—is not relevant because it is sufficient that the foreign government's intrusive activities occurred on US territory. It can be safely assumed that the confidential data of 22.1 million US government employees was stored on servers within the US. If the allegations are correct, China was thus guilty of violating the US's territorial sovereignty.

II. Intervention in Another State's Affairs

The same cannot be automatically assumed for the Democrats' hacked emails, as it remains unclear where they were stored or obtained from. This reinforces the limitations of the territorial sovereignty argument outlined above with respect to the legality of cyber espionage. The servers on which emails were stored were likely located in many States and not necessarily in the State from which the emails originated. Furthermore, government or party officials may send emails while they travel abroad, thereby accessing their emails from abroad, which would also involve servers located in other States. This is even more pronounced when data is stored in one of the many available clouds. Furthermore, emails sent and received within the boundaries of one State are sometimes routed via servers in another State.[13] To complicate the situation further, some States have the capacity to monitor internet communications in real time.[14]

[10] Islands of Palmas Case (Neth. v. U.S.), 1928 R.I.A.A. 829, 838 (1928).

[11] The Case of the S. S. "Lotus" (Fr. V. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

[12] For the purposes of the discussion here, it is irrelevant whether the alleged cyber espionage was undertaken by government officials or by private actors at the Russian/Chinese governments' behest.

[13] Patrick Beuth, *NSA Kann Drei Von Vier E-Mails Mitlesen*, DIE ZEIT (Aug. 21, 2013), http://www.zeit.de/digital/datenschutz/2013-08/nsa-ueberwacht-75-prozent-internet; Charles Arthur, *NSA-Scandal: What Data Is Being Monitored and How Does It Work?*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions.

[14] Glenn Greenwald, *XKeyscore: NSA Tools Collect "Nearly Everything a User Does on the Internet"*, THE GUARDIAN (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; *NSA Sucks Realtime Data from Fifty Companies*, DAILY MAIL (June 9, 2013), http://www.dailymail.co.uk/news/article-2338367/NSA-sucks-realtime-data-FIFTY-companies.html.

Thus, the location of data obtained at the time of an email hack often cannot be determined with precision. The way internet services are provided makes it almost impossible for a State to justifiably accuse another State that has engaged in this sort of cyber espionage of violating its territorial sovereignty. The situation is therefore entirely comparable to the one decided by the ECHR when it negated a violation of sovereignty.

It follows that it is necessary to examine whether other prohibitive rules of public international law could be implicated by such cyber espionage conduct. The prohibition on interventions in the internal affairs of another State is a likely candidate. It is widely agreed that this prohibition has developed into a rule of customary international law.

According to Article 8 of the Montevideo Convention, "no [S]tate has the right to intervene in the internal or external affairs of another."[15] Following WWII, numerous international instruments have repeatedly confirmed this rule of customary international law. Article 2(7) of the UN Charter rules out any intervention by the UN in a member State's internal affairs.[16] Article 19 of the OAS Charter similarly stated:

> 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. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic, and cultural elements.[17]

By the 1960s, broad international consensus on the prohibition of intervention in another State's internal affairs had developed. In 1965, the General Assembly passed the *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty* in a 109:0:1 vote.[18] It stated, *inter alia*, that

> No State 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

[15] Montevideo Convention on the Rights and Duties of States, Dec. 26, 1933, 165 L.N.T.S. 19.

[16] U.N. Charter art. 2, para. 7.

[17] Charter of the Organization of American States, Apr. 30, 1948, 119 U.N.T.S. 47; *see also* Treaty of Friendship, Cooperation and Mutual Assistance art. 8, May 14, 1955, 219 U.N.T.S. 23.

[18] G.A. Res. 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty (Dec. 21, 1965).

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

> attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned.[19]

In 1970, the General Assembly reaffirmed these statements in its *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States,* which was passed without a vote: "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."[20]

Although these resolutions were not legally binding, the fact that they passed by consensus, with the latter Declaration explicitly referring to international law, supports the conclusion that States viewed the content of the Declaration as being reflective of their interpretation of the international legal rules. It is therefore justified to view the prohibition on intervention in the internal or external affairs of another State as a rule of customary international law.[21] In 2005, the ICJ in fact confirmed that the *Friendly Relations Resolution* was "declaratory of international law."[22] The ICJ itself has also repeatedly stressed the legal quality of the prohibition of such interventions. By 1949, the Court had already expressly declared interventions in other States' affairs to be unlawful.[23]

However, it is the ICJ's 1986 Nicaragua judgment that is often referred to when discussing the prohibition on interventions, probably because the court attempted to provide at least a partial definition of the prohibition's content:

> The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law.[24]

---

[19] *Id.*

[20] G.A. Res. 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Oct. 24, 1970).

[21] Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SECURITY L. & POL'Y 179, 198 (2011); Aaron Shull, *Cyberespionage and International Law*, *in* GIGANET 8TH ANNUAL SYMPOSIUM 1, 3–4 (2013).

[22] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, para. 162 (Dec. 19).

[23] U.K. v. Alb., 1949 I.C.J. at 34–5.

[24] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. 14, para. 202 (June 27); *see also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgement, 2005 I.C.J. 168, at paras. 161–65 (Dec. 19).

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful *when it uses methods of coercion* in regard to such choices, which must remain free ones.[25]

The reference to "methods of coercion" is often claimed to limit the scope of the prohibition. Many argue that this restriction is especially relevant in relation to cyber espionage. Collecting secret information remotely—for example, by hacking emails—is seen by many as lacking the necessary coercive element, thus failing to meet the threshold of prohibited intervention.[26]

For various reasons, this line of argument is not convincing. First of all, it overlooks the fact that the ICJ stressed that it was only looking at "those aspects of the principle which appear to be relevant" to the case before it.[27] As the court was dealing with the US's massive support of the Nicaraguan rebels, the *Contras*, who were attempting to overthrow their country's government by force, it was not necessary for the court to explore the issue of "coercion" in any detail. The US's involvement in the rebels' use of force in their quest to take power,

---

[25] Nicar. v. U.S., 1986 I.C.J. at para. 205 (emphasis added); *see also* Shull, *supra* note 21, at 4.

[26] Kirstin Schmalenbach, CASEBOOK INTERNATIONALES RECHT, 29–30 (2nd ed. 2014); Helmut P. Aust, *Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014*, HU BERLIN 16 (2014), https://www.bundestag.de/blob/282870/fc52462f2ffd254849bce19d25f72fa2/mat_a_sv-4-1_aust-pdf-data.pdf; Anne Peters, *Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I*, EJIL: TALK! (Nov. 1, 2013), https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/; Shoshan, *supra* note 1, at 43–5; Stefan Talmon, *Sachverständigengutachten gemäß Beweisbeschluss SV-4 des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode*, UNIVERSITÄT BONN 20–21 (2014), https://www.bundestag.de/blob/282872/2b7b605da4c13cc2bc512c9c899953c1/mat_a_sv-4-2_talmon-pdf-data.pdf. Talmon also bases his view on the ICJ's reasoning in the *Nicaragua Case*. When dealing with unauthorized fly overs by US planes over Nicaraguan territory, the court concluded that such conduct violated Nicaragua's sovereignty but did not deal with the question of whether these flights also amounted to an unlawful intervention. This argument is unconvincing. The ICJ had no reason to examine whether these reconnaissance flights constituted an unlawful intervention or not. Nicaragua claimed that its sovereignty had been violated by the flights and the court concurred. Therefore, there was no need for the court to further examine US conduct. *See* Nicar. v U.S., 1986 I.C.J. at paras. 87–91, 251; Stefan Talmon, *Das Abhören des Kanzlerhandys und das Völkerrecht*, 1 BONNER RECHTSJOURNAL 6, 10 (2014). *See also* Torsten Stein& Thilo Marauhn, *Völkerrechtliche Aspekte von Informationsoperationen*, 60 ZAÖRV 1, 22–5 (2000) (providing a more general discussion of the difficulty of distinguishing between acceptable "persuasion" of another State and "coercion").

[27] Nicar. v. U.S., 1986 I.C.J. at para. 205; *see also* Shull, *supra* note 21, at 4.

without any reference to the population's wishes, was without a doubt "coercive" in nature as far as Nicaragua's "choice of a political . . . system" was concerned.

Nevertheless, it does not follow that relatively less coercive means are therefore automatically permissible. Correctly understood, it would rather seem that the difference between coercive intervention and potentially permissible interference in another State's affairs comes down to whether the target State retains its freedom of choice in matters related to its sovereign rights. An intervention is thus unlawful when the target State risks losing its freedom to act on an issue related to its internal or external affairs. Actions below that threshold, aiming at persuasion rather than compulsion, may well be permissible.

Applying this understanding of unlawful intervention to cyber espionage suggests that obtaining secret government information—even remotely—is prohibited under public international law. It is self-evident that it is a State's prerogative and sovereign right, as part of its foreign and domestic policy, to decide what information it shares with other States, whether they are allies or foes. A sovereign government has the right to develop its domestic and foreign affairs policies unobserved by a foreign power, and to protect its relationship with its employees. A sovereign State also has the right to decide whether it wants to share information with other States. And yet, Russia and, or China seem to have forced the US into unwittingly disclosing what it, as a sovereign State, had decided not to disclose. The US was thus robbed of the opportunity to make a sovereign decision on who it wanted to share information like the details of 22.1 million of its employees with.[28] This is sufficient to meet the coercion threshold of unlawful intervention.

Admittedly, the emails allegedly hacked by the Russians did not originate from within the US government, but from a political party. Nevertheless, collecting secret information should not be assessed separate from the motives for doing so.[29] Some argue that the reason for collecting information may well be incompatible with international law, but that this does not touch upon whether the collection as such was unlawful under public international law.[30] Yet, there is no reason to *always* treat a spying State's motives as irrelevant to assessing the lawfulness of subsequent actions. To be sure, it is self-evidently true that a

[28] Shoshan, *supra* note 1, at 45–7; Shull, *supra* note 21, at 6–7; Pål Wrange, *Intervention in National and Private Cyberspace and International law,* STOCKHOLM FACULTY OF L. RESEARCH PAPER SERIES NO. 23 8–9 (2017). However, Wrange bases this analysis on the assumption that the agent, even when operating remotely from his own country, is violating the domestic laws of the target State, which in turn allows the author to conclude that the agent is guilty of an illegal intervention. Schmalenbach, *supra* note 26, at 30 (mentioning the same argument but leaving it open to question whether the author agrees with it).

[29] Richard A. Falk, *Space Espionage and World Order: A Consideration of the Samos-Midas-Program*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 45, 58 (Quincy Wright *et al* eds.); Alison Pert, *Australia's Jakarta Phone-Tapping: Was it Illegal?*, INSIDE STORY (Nov. 27, 2013), http://insidestory.org.au/australias-jakarta-phone-tapping-was-it-illegal; Shull, *supra* note 21, at 5.

[30] Schmalenbach, *supra* note 26, at 30; Shoshan, *supra* note 1, at 45.

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

State's motives may sometimes not be decisive when judging whether a specific action was lawful under public international law.[31] But, there are also cases where the opposite is true. A State's armed response to an armed attack will be judged differently based on whether that response was defensive in nature—lawful self-defense—or punitive—unlawful reprisal.[32] Similarly, an intervention seemingly justified on the grounds of the controversial doctrine of humanitarian intervention or the Responsibility to Protect may only be seen as a lawful intervention if it was motivated by humanitarian concerns.[33]

As far as collecting secret information against another's State wishes in order to influence that State's foreign policy or gain an upper hand in negotiations with that State, there is every reason to consider the spying State's motives when assessing the legality of the monitoring activity.[34] Obviously, it would be unrealistic to assume that a State collecting another State's secret information will not do more than file it away. A State that spies on another State may do so to thwart the other's foreign policy initiatives that it views as contrary to its own national interest. It may likely pursue this by exerting pressure on politicians or government employees to make them change their minds or to provide further secret information. To that end, it is easily imaginable that private information on foreign politicians or government personnel might prove useful to a State wanting to persuade such persons to adopt a more amenable view on issues of foreign and trade policy, possibly even by means of blackmail. Why else would the Chinese government be interested in acquiring the data of 22.1 million US government employees? Such action would therefore undoubtedly contain the coercive element necessary to illegal intervention in another State's internal affairs.[35] The collection of secret information thus cannot be judged

---

[31] Aerial Incident of 3 July 1988 (Iran v. U.S.), Memorial Submitted by the Islamic Republic of Iran 197–204 (July 24, 1990), http://www.icj-cij.org/files/case-related/79/6629.pdf (noting that the Memorial mentions many incidents when the accused State's motives were viewed as irrelevant to the assessment to the legality of that State's actions).

[32] CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 203 (3d ed. 2008); ANTONIO CASSESE, INTERNATIONAL LAW 299–302 (2d ed. 2005); W. Michael Reisman, *The Raid on Bagdad: Some Reflections on its Lawfulness and Implications* 5 EUR. J. INT'L L. 120 (1994).

[33] *See, e.g.*, U.N. Secretary-General, *Implementing the Responsibility to Protect*, U.N. Doc. A/63/677, (Jan. 12, 2009).

[34] Pert, *supra* note 29, at 2; Stein, *supra* note 26, at 24; Christoph D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1097 (2003).

[35] *See, e.g.*, Martin Bright, Ed Vulliamy & Peter Beaumont, *Revealed: US Dirty Tricks to Win Vote on Iraq*, THE GUARDIAN (Mar. 2, 2003), http://www.theguardian.com/world/2003/mar/02/usa.iraq. The authors refer to a memo describing the US spying on UN diplomats that represent then-sitting States of the Security Council. The authors further explain that:

> The memo is directed at senior NSA officials and advises them that the agency is "mounting a surge" aimed at gleaning information not only on how delegations on the Security Council will vote on any second resolution on Iraq, but also "policies," "negotiating positions," "alliances" and "dependencies"—the "whole gamut of information

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

separately from the State's motives; rather, cyber espionage must consequently be seen as the initiation of illegal intervention in another State's affairs and, accordingly, as an indispensable and enabling part of that intervention.

As far as the allegations against Russia are concerned, this is even more self-evident. If Russia was indeed responsible for hacking and publishing emails circulating among the leadership of the Democrats, it is and should be relevant that this was done to influence the outcome of the US Presidential election. Cyber espionage was employed to intervene in the electoral process. The democratic election of a State's leadership is definitely an issue that is extremely relevant to any concept of "sovereignty." A State that attempts to manipulate public opinion to undermine the election of officials of another State by way of cyber espionage is guilty of intervening in the internal affairs of that State. As Craig Forcese has pointed out,[36] the *Tallinn Manual*, which generally remains more hesitant in assuming the unlawfulness of an intervention in cases of cyber espionage, confirms as much:

> Acts meant to achieve regime change are often described as a clear violation. So too is coercive "political interference." When such actions are taken or facilitated by cyber means, they constitute prohibited intervention. Cases in point are the manipulation by cyber means of elections or of public opinion on the eve of elections . . . .[37]

Therefore, it can be concluded that hacking emails circulating among the Democratic leadership was contrary to public international law because it amounted to a prohibited intervention into the internal affairs of the United States.

> that could give US policymakers an edge in obtaining results favourable to US goals or to head off surprises."

Id.

[36] Craig Forcese, *The "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?*, JUST SECURITY (Dec. 16, 2016), https://www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/.

[37] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 45 (Michael N. Schmitt ed., 2013).

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

C. Clean-Hands-Principle

Some have argued that the "clean-hands-principle"[38] makes any claim of illegal espionage by one State against another State untenable when all States are guilty of espionage against other States.[39] This argument would also apply to cyber espionage, as all States that have the capacity to do so will most likely engage in it. In the case of the US this became publicly known through the Snowden revelations, which uncovered massive cyber espionage operations by the National Security Agency (NSA).[40]

Whether the clean-hands-principle has actually developed into a rule of customary international law—as a wholesale preclusion or as a factor in assessing the admissibility of a claim put forward by an injured State—is contentious.[41] It is also generally agreed that the clean-hands-principle, if it exists in any form, can only be invoked by the offending State if the reciprocal conduct is comparable in "nature and gravity."[42] With regard to China, it is not publicly known whether the Chinese government would be justified in putting forth a claim based on US cyber espionage activities against China. The same applies to Russia. Nevertheless, based on the Snowden revelations, which indicated that the NSA engaged in worldwide monitoring of internet communications, the possibility that Russia or China would rely on such a counter-claim cannot be ruled out.

The situation is similarly nebulous as concerns US interference in Russia's electoral process. There certainly have been many instances in the past when the US has been accused of massive interference in other countries' elections. According to Don Levin, the US

[38] A definition was provided by Judge Hudson in his *Individual Opinion* in the *River Meuse* Case before the PCIJ: "It would seem . . . that where two parties have assumed an identical or a reciprocal obligation, one party which is engaged in a continuing non-performance of that obligation should not be permitted to take advantage of a similar non-performance of that obligation by the other party." *See* Diversion of Water from the River Meuse (Neth. v. Belg.), Judgement, 1937 P.C.I.J. (ser. A/B) No. 70, at para. 323 (June 28).

[39] Schmalenbach, *supra* note 26, at 30–4 (mentioning this and some closely related arguments); JORGE H. ROMERO, CYBERESPIONAGE 2010: IS THE CURRENT STATUS OF ESPIONAGE UNDER INTERNATIONAL LAW APPLICABLE IN CYBERSPACE? 19 (Storming Media 2011).

[40] GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014); MARCEL ROSENBACH & HOLGER STARK, DER NSA KOMPLEX (2015).

[41] James Crawford (Special Rapporteur), *Second Report on State Responsibility*, para. 330–34, U.N. Doc. A/CN.4/498/Add.2 (Apr. 30, 1999); JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 701 (8th ed., 2012).

[42] Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* 3 ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 21 (Quincy Wright *et al* eds., Leopold Classic Library, 1962); Schmalenbach, *supra* note 26, at 30–4.

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

intervened in elections of other States on more than 80 occasions between 1946 and 2000.[43] With regard to Russia, it is alleged that the US intervened in the 1996 presidential election in order to save the West's preferred candidate, Boris Yeltsin, from near-certain defeat.[44] Furthermore, the Russians have accused the US of attempting to influence the outcome of the 2011 parliamentary elections, singling out for particular criticism the then-Secretary of State, Hilary Clinton.[45]

Against this backdrop, and provided the clean-hands-principle were accepted as a valid defense, which as has been pointed out is doubtful, the successful invocation of the principle by China or Russia cannot be ruled out.

D. Conclusion

This short Article has examined the question of whether the alleged Russian interference in the US electoral process and the alleged Chinese theft of personnel data of US government employees by means of cyber espionage was unlawful under public international law.

I have argued that obtaining secret or confidential government data stored on servers located on US territory violates US territorial sovereignty and is therefore unlawful. As the secret information obtained on US government employees was most likely stored on servers on US territory, Chinese access to this data via cyber espionage amounted to the exercise of Chinese governmental authority in the US without the consent of the latter. Therefore, Chinese conduct in this respect was impermissible.

As far as hacking the emails of the Democrat leadership, the issue is more complex. It was shown that it cannot be blithely assumed that these emails were accessed on US territory. Thus, it is more difficult to sustain an accusation of a violation of territorial sovereignty. Further complicating the matter is that the emails did not originate from official government sources. Nevertheless, I argued that the legality of cyber espionage is tied to the spying State's motives for doing so. If, as it seems, Russia was attempting to influence the outcome of the US presidential elections, there can be no doubt that hacking and publishing the DNC emails was an unlawful intervention in the US's internal affairs.

---

[43] Nina Agrawal, *The US is No Stranger to Interfering in the Elections of Other Countries*, LOS ANGELES TIMES (Dec. 21, 2016), http://www.latimes.com/nation/la-na-us-intervention-foreign-elections-20161213-story.html.

[44] Agrawal, *supra* note 43; Markar Melkonian, *US Meddling in 1996 Russian Elections in Support of Boris Yeltsin*, GLOBAL RESEARCH (Jan. 13, 2017), http://www.globalresearch.ca/us-meddling-in-1996-russian-elections-in-support-of-boris-yeltsin/5568288.

[45] Robert Bridge, *Election-meddling Fiasco Hits US-Russia Relations*, RUSSIA TODAY (Dec. 9, 2011), https://www.rt.com/politics/russia-us-elections-clinton-putin-2012-usaid-427/.

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press

Nevertheless, the fact that the US itself stands accused of massive cyber espionage operations to the disadvantage of many other States, including allied States, cannot be ignored. It is not unlikely that the US is conducting cyber espionage operations against both Russia and China. Similarly, the US has frequently been accused of meddling in other States' elections, including Russia's. Regardless of whether the clean-hands-principle has become a rule of customary international law, the fact the US engages in such activities undermines its claims against both States and allows others to accuse it of hypocrisy.

As cyber espionage is slowly becoming one of the most prominent ways of illicitly obtaining the secret information of other States, an international agreement on the topic is highly desirable. As unlikely as such an agreement was at a time when the US was the dominant player in cyber espionage, creating such a body of rules may meet less resistance by the US now that it has become the victim of massive cyber espionage with potentially far-reaching consequences. Certainly, it is far from convincing if the US continues to accuse other States of unlawful interference by means of cyber espionage while at the same time engaging in identical activities. This "Don't Do as I Do" approach is no longer acceptable.

https://doi.org/10.1017/S207183220002280X Published online by Cambridge University Press