Radosław Fordoński
Uniwersytet Warmińsko-Mazurski w Olsztynie
Wojciech Kasprzak
Uniwersytet Warmińsko-Mazurski w Olsztynie

Alleged Russian interference in the 2016 US presidential election and prohibition of non-intervention

Introduction

Cyber intervention,[1] like its physical counterpart, could take various forms and reach varying degrees of intensity. It could be used to break into sensitive governmental and other critical websites with the purpose of interfering with governmental communications, manipulating key economic and financial activities, or planting malware designed to degrade or shut down essential governmental and other key services at a moment of the intervening State's choosing.

It could include various forms of misinformation and propaganda aimed at undermining a foreign government's legitimacy and escalating to incitement and coordination of subversive activity, with the purpose of aggravating civil unrest or even overthrowing a foreign government. The (mis)use of social media, email and digital telephone communications for such purposes could be a potentially powerful instrument in inciting or assisting opposition to an unfriendly foreign government, especially in countries which were subject to significant civil unrest as a result of political, social or other types of instability. Finally, it could be used to manipulate or influence the outcome of elections in States where polling was (partially) conducted through digital voting procedures.[2]

[1] Cyber intervention is defined as "a violation of the principle of nonintervention which is carried out wholly, or at least predominately, in the cyber domain. Consequently, it must rise to the level of illegal coercive activity which attempts to prevent a State from conducting its domestic affairs and foreign relations in conformity with its own choices within the limits of international law." See T. D. Gill, 'Non-Intervention in the Cyber Context', in: K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013) 217–238, 232.

[2] Ibidem, 234.

Permissibility of the last type of intervention under international law is discussed in the following analysis. Its factual context is constituted by the case-study of a alleged Russian intereference in the 2016 US presidential election.

To the layperson, the Russian hacking constituted an impermissible (and perhaps) shocking interference in the American political process-an intervention that nonlawyers would not hesitate to label a "violation of sovereignty" as that term is used in political or diplomatic discourse. The problem arises when one attempts to translate that common sense intuition into legal discourse.

All official statements by the US administration appear to include a "studied avoidance" of whether the Russian actions do or do not violate international law.[3] Note this conspicuous line in the President's statement on 29 December 2016, concerning Washington's response to "certain cyber activity that seeks to interfere with or undermine our election processes and institutions": "These actions … are a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior."[4]

As R. Goodman comments on this statement:

"Political scientists talk about "international norms of behavior"—for international lawyers, on the other hand, such terms do not connote an international legal obligation. It is safe to assume the specific word choice in the President's statement is highly deliberate."[5]

The administration had another opportunity recently to label action like the Russian DNC hack a violation of international law, but didn't. Two days after the 8 November 2016 presidential election, the State Department's Legal Adviser Brian Egan gave an important speech on cyber and international law. In discussing this area of law, he said:

"In certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law, even if it falls below the threshold of a use of force. (...) For example, a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention."[6]

---

[3] R. Goodman, 'International Law and the US Response to Russian Election Interference', Just Security, 5 January 2017, available at: https://www.justsecurity.org/35999/international-law-response-russian-election-interference/ (accessed 5 September 2018).

[4] White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, 29 December 2016, available at: https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (accessed 30 December 2016).

[5] Goodman, 'International Law and the US Response to Russian Election Interference', *supra* note.

[6] B. J. Egan, 'Remarks on *International Law and Stability in Cyberspace*, Berkeley Law School, (*November 10, 2016)*', (2017) 35(1) Berkeley JIL (Berkeley Journal of International Law) 169–180, 174–175.

While giving two examples of "clear" violations the Egan speech does not set the outer limits of what action would violate the relevant legal rule, leaving open the legal question may boil down to whether an operation intended to cast grave public doubt on the integrity of the results would count, or if the Egan speech is meant instead to refer to altering the actual outcome.[7]

On the other hand, a joint intelligence assessment prepared by the National Security Agency, Central Intelligence Agency and Federal Bureau of Investigation states that while

"Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[8]

In order to verify both contradictory claims under principle of non-intervention as recognized in treaty and customaty international law, the following analysis is divided into three parts.

First, it presents scope an cursory assessment of the alleged Russian interference in the 2016 US presidentional election the the preceding campaign. Then the substantive content and scope of the principle of non-intervention is briefly set out. The final section involves assessment of legality of election cyberinterference under legal parameters established in the preceding part of the analysis.

---

[7] Goodman, 'International Law and the US Response to Russian Election Interference', *supra* note. See also R. Crootof, 'The DNC Hack Demonstrates the Need for Cyber-Specific Deterrents', Lawfare, 9 January 2017, available at: https://www.lawfareblog.com/dnc-hack-demonstrates-need-cyber-specific-deterrents (accessed 3 September 2018) ("Despite the U.S. response "being the strongest public action the United States has ever taken in response to a cyberoperation, the Obama's administration actions have been derided as "too little, too late", "confusing and weak", and "insufficient". However, this seemingly insufficient reaction "may have been informed by international law; the United States might have responded to the DNC hack as it did because international law did not permit it to do more."). But see D. Hollis, 'Russia and the DNC Hack: What Future for a Duty of Non-Intervention?', Opinio Juris, 25 July 2016, available at: http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/ (accessed 5 September 2018) ("I'm not so sure, however, that the duty of non-intervention can be dismissed so quickly. (...) Perhaps we need to separate out this incident into two parts – the espionage (i.e., the hack itself) and the interference in the U.S. campaign using the fruits of that espionage. (...) Interference in 'any form' is clearly a broader formulation than coercive acts, suggesting that actions designed to impact public support for not just a particular candidate, but an entire "political" party, could implicate the duty of non-intervention here.").

[8] Assessing Russian Activities and Intentions in Recent US Elections', Intelligence Community Assessment No. ICA 2017-01D, 6 January 2017, available at: https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf (accessed 20 June 2018), ii.

1. Alleged Russian intereference in 2016 US presidential campaign and election

Russian cyber operation targeting the 2016 election was multifaced.[9] The following presentation includes:
– cyberespionage against US political organizations;
– public disclosures of data obtained through covert intelligence activities;
– overt propaganda by state-funded media;
– cyberintrusions into US state and local electoral boards; and
– "fake news" influence efforts in social media.

1.1. Cyberespionage against US political organizations

First of all, Russia used two cyberespionage teams of a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU") to hack into computers and email systems in the 2016 US election. Additionally, we know that Russian cyberespionage teams took some of the information it found in these computers and systems, because some of the information and emails it discovered through unauthorized access were later published.

The GRU Unit 26165 – colloquially known as "Cozy Bear" or "APT 29" – and dedicated to targeting military, political, governmental, and non-governmental organizations with spearphishing emails and other computer intrusion activity, hacked computers at the Democratic National Committee ("DNC") and penetrated the email account of Clinton's presidential campaign chair, John Podesta during 2015 and 2016.[10] Russia also hacked the Republican National Committee ("RNC") emails using a Unit 74455 called "Fancy Bear," or "APT 28"[11].

In addition, Russia conducted a massive operation to target US primary campaigns, think tanks, and lobbying groups they viewed as likely to shape future US policies[12].

1.2. Public disclosures of data obtained through covert intelligence activities

Second, Russia selectively disseminated some of the hacked emails.

Initially, Russian intelligence officials posted them to WikiLeaks and other websites on 22 July 2016. This leak included nearly 20,000 emails and

[9] Ibidem, 2.

[10] *U.S. v. Viktor Borisovich Netyksho, et al*, Indictment of 13 July 2018, available at: https://www.justice.gov/file/1080281/download (accessed 3 September 2018), paras. 10, 13, 21.

[11] J. Van De Velde, 'The law of Cyber Interference in Elections', SSRN, 15 May 2017, available at: https://ssrn.com/abstract=3043828 (accessed 3 August 2018), 11.

[12] 'Assessing Russian Activities and Intentions in Recent US Elections', *supra* note, 2.

8,000 attachments that belonged to seven top officials at the DNC. While most of the emails were innocuous, a number of them confirmed that the DNC favored presidential candidate Hillary Clinton over Bernie Sanders, causing outrage due to the DNC's professed neutrality regarding the Democratic Party nominee.[13] In the technology community, this type of leak is known as "organizational doxing", and involves "hackers, in some cases individuals- and in others nation-states, [who] are out to make political points by revealing proprietary, secret, and sometimes incriminating information (...) airing the organizations' embarrassments for everyone to see."[14]

The 22 July doxing took place three days before the Democratic Party Convention in Philadelphia,[15] where there were rumors that already-dissatisfied supporters of Bernie Sanders might attempt to derail the official nomination process (indeed, subsequent events included organized protests against the DNC and the resignation of DNC Chairwoman Debbie Wasserman Schultz)[16].

The second batch (8,000 emails) was released on 6 November 2016, two days before the election. The third batch of emails released by WikiLeaks belonged to Podesta, the chairman of Clinton's presidential campaign and a former White House chief of staff. The emails were obtained by sending a spear-phishing email to Podesta's Gmail account in March 2016. The Podesta emails contained evidence of controversial remarks that Clinton gave to various Wall Street audiences, including Goldman Sachs bankers, lending credibility to the damaging accusation that she maintained a cozy relationship with the financial sector. This leak occurred on the same day the White House accused Russia of orchestrating the DNC hack.

The timing of each wave appeared strategic. July and November release dates corresponded closely to known inflection points in the campaign, when public attention was at its zenith and dissatisfied Democrats would be most prone to be affected by negative information about Clinton and the DNC's perceived manipulation of the primary process. Podesta emails were then published on 7 October 2016, a mere hour after the Washington Post released the *Access Hollywood* tape of Donald Trump making degrading comments about women. The timing of the release, and its favorability to Trump, reinforced suspicion that Russia supported the Republican candidate[17].

---

[13] In addition, many emails included information pertaining to the party's donors, their credit card details, Social Security numbers, and other personal information. Kilovaty, 'Doxfare', *supra* note, 156.

[14] I. Kilovaty, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information', (2018) 9 Harvard NSJ (Harvard National Security Journal) 146–179, 149.

[15] *U.S. v. Viktor Borisovich Netyksho,et al, supra* note , para. 48.

[16] Kilovaty, 'Doxfare', *supra* note, 149, 155.

[17] Kilovaty, 'Doxfare', *supra* note, 155–156.

At the same time Russia collected on some Republican-affiliated targets but did not conduct a comparable disclosure campaign.[18] In other words, RNC emails hacked by the GRU Unit 74455 were not disseminated[19].

Russian dissemination of information arguably had significant impact on congressional races, and citizen trust in the democratic process more generally. The fallout from the dissemination of DNC emails was immediate. Wasserman Schultz, the chair of the D.N.C., was forced to resign, along with her top aides. On the state level, confidential documents taken from the Democratic Congressional Campaign Committee relating to congressional races in a dozen states were published, tainting many affected races with accusations of scandal[20].

1.3. Overt propaganda by state-funded media

Russia also engaged in "information warfare" campaigns. Sites like RT News and Sputnik, both state-funded Russian sites, shared anti-US propaganda, contributing to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences[21].

---

[18] 'Assessing Russian Activities and Intentions in Recent US Elections', *supra* note, 3.

[19] Van De Velde, 'The law of Cyber Interference in Elections', *supra* note, 11.

[20] Ibidem, 11–12.

[21] The notion of "information warfare" was used byRT Editor in Chief Margarita Simonyan herself when she characterized 2012 RT's coverage of the Occupy Wall Street movement as aimed at promoting popular dissatisfaction with the US Government. In an earlier example of RT's messaging in support of the Russian Government, during the Georgia-Russia military conflict the channel accused Georgians of killing civilians and organizing a genocide of the Ossetian people. According to Simonyan, when "the Ministry of Defense was at war with Georgia", RT was "waging an information war against the entire Western world." The Kremlin spends $190 million a year on the distribution and dissemination of RT programming, focusing on hotels and satellite,terrestrial, and cable broadcasting. Simonyan admits that the Russian Government sets rating and viewership requirements for RT and, "since RT receives budget from the state, it must complete tasks given by the state." RT news stories are written and edited "to become news" exclusively in RT's Moscow office. Simonyan has close ties to top Russian Government officials, especially Presidential Administration Deputy Chief of Staff Aleksey Gromov, who reportedly manages political TV coverage in Russia and is one of the founders of RT. Simonyan replaced Gromov on state-owned Channel One's Board of Directors. Government officials, including Gromov and Putin's Press Secretary Peskov were involved in creating RT and appointing Simonyan. According to Simonyan, Gromov oversees political coverage on TV, and he has periodic meetings with media managers where he shares classified information and discusses their coverage plans. In addition, the head of RT's Arabic-language service, Aydar Aganin, was rotated from the diplomatic service to manage RT's Arabic-language expansion, suggesting a close relationship between RT and Russia's foreign policy apparatus. RT's London Bureau is managed by Darya Pushkova, the daughter of Aleksey Pushkov, the current chair of the Duma Russian Foreign Affairs Committee and a former Gorbachev speechwriter. In her interview with pro-Kremlin journalist Sergey Minaev, Simonyan complimented RT staff in the United States for passionately defending Russian positions on the air and in social media. Simonyan said: "I wish you could see…how these guys, not just on air, but on their own social networks, Twitter, and when giving interviews, how they defend the positions that we stand on!" See 'Assessing Russian Activities and Intentions in Recent US Elections', *supra* note, 9–10.

State-owned Russian media made increasingly favorable comments about President elect Trump as the 2016 US general and primary election campaigns progressed while consistently offering negative coverage of Secretary Clinton. Starting in March 2016, Russian Government-linked actors began openly supporting President-elect Trump's candidacy in media aimed at English-speaking audiences. RT and Sputnik, another government-funded outlet producing pro-Kremlin radio and online content in a variety of languages for international audiences, consistently cast President-elect Trump as the target of unfair coverage from traditional US media outlets that they claimed were subservient to a corrupt political establishment. Russian media hailed President-elect Trump's victory as a vindication of Putin's advocacy of global populist movements – the theme of Putin's annual conference for Western academics in October 2016 – and the latest example of Western liberalism's collapse.

Putin's chief propagandist Dmitriy Kiselev used his flagship weekly newsmagazine program in 2016 fall to cast President-elect Trump as an outsider victimized by a corrupt political establishment and faulty democratic election process that aimed to prevent his election because of his desire to work with Moscow. Pro-Kremlin proxy Vladimir Zhirinovskiy, leader of the nationalist Liberal Democratic Party of Russia, proclaimed just before the election that if President-elect Trump won, Russia would "drink champagne" in anticipation of being able to advance its positions on Syria and Ukraine.

At the same time RT's coverage of Secretary Clinton throughout the US presidential campaign was consistently negative and focused on her leaked e-mails and accused her of corruption, poor physical and mental health, and ties to Islamic extremism. Some Russian officials echoed Russian lines for the influence campaign that Secretary Clinton's election could lead to a war between the United States and Russia.

In August 2016, Kremlin-linked political analysts suggested avenging negative Western reports on Putin by airing segments devoted to Secretary Clinton's alleged health problems.

On 6 August, RT published an English language video called "Julian Assange Special: Do WikiLeaks Have the E-mail That'll Put Clinton in Prison?" and an exclusive interview with Assange entitled "Clinton and ISIS Funded by the Same Money." RT's most popular video on Secretary Clinton, "How 100% of the Clintons' 'Charity' Went to…Themselves," had more than 9 million views on social media platforms. RT's most popular English language video about the President-elect, called "Trump Will Not Be Permitted To Win," featured Assange and had 2.2 million views[22].

[22] Ibidem, 3–4.

1.4. Cyberintrusions into US state and local electoral boards

Russia allegedly targeted the voter registration systems in over 20 state election systems. Four of the twenty systems were, in fact, breached[23].

Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment to identify vulnerabilities, accessing elements of multiple state or local electoral boards. Although the types of systems Russian actors targeting or compromising were not involved in 2016 vote tallying,[24] stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers[25].They also hacked into computers of a company that supplied software used to verify voter registration information,[26] targeted state and local offices responsible for administering the elections and sent spearphishing emails to people involved in administering elections, with malware attached[27].

The US Department of Justice tressed, however, that the indictments contained "no allegation that the conspiracy altered the vote count or changed any election result."[28] On the other hand, the US intelligence community has not attempted to assess the misinformation campaign's influence on individual voter choice. As stated by the former US Director of National Intelligence, James Clapper, there is "no way of gauging the impact [the operation had] on choices the electorate made". The current US administration has not altered this assessment[29].

1.5. "Fake news" influence efforts in social media

Thes abovementioned activities were exacerbated by a coordinated campaign over social media platforms to highlight these disclosures, spread false stories and delegitimize the US government. The campaign was conducted

---

[23] Van De Velde, 'The law of Cyber Interference in Elections', *supra* note, 12.

[24] 'Assessing Russian Activities and Intentions in Recent US Elections', *supra* note, 3.

[25] *U.S. v. Viktor Borisovich Netyksho, et al, supra* note, para. 72. D. Trump won the 2016 election by winning three key states (Ohio, North Carolina and Pennsylvania) by slim margins that added up to around 80,000 votes. C. Wilkie, '5 key takeaways from the latest indictment in Mueller's Russia probe', CNBC online edition, 13 July 2018, available at: https://www.cnbc.com/2018/07/13/5-key-takeaways-from-mueller-indictment-of-russian-election-hackers.html (accessed 4 September 2018).

[26] *U.S. v. Viktor Borisovich Netyksho,et al, supra* note , para. 73.

[27] US Department of Justice, Deputy Attorney General Rod J. Rosenstein Delivers Remarks Announcing the Indictment of Twelve Russian Intelligence Officers for Conspiring to Interfere in the 2016 Presidential Election Through Computer Hacking and Related Offenses, 13 July 2018, available at: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-announcing-indictment-twelve (accessed 4 September 2018).

[28] Ibidem.

[29] Russian Meddling in Elections and referenda in the Alliance, *supra* note, para. 26.

by a designated organization created "to engage in operations to interfere with elections and political processes."[30] The Internet Research Agency was founded in July 2013 and has been funded since to the tune of $15 million a year, with a contingent of hundreds of staffers by 2016 and bonuses running to the hundreds of thousands of dollars[31]. With a "strategic goal to sow discord in the US political system" its employees made various expenditures to carry out those activities, including buying political advertisements on social media in the names of US persons and entities. Defendants also staged political rallies inside the United States, and while posing as US grassroots entities and US persons, and without revealing their Russian identities and affiliation, solicited and compensated real US persons to promote or disparage candidates. Some defendants, indicted in February 2018, communicated with unwitting individuals associated with the campaign of Donald Trump and with other political activists to seek to coordinate political activities, also posing as US persons and without revealing their Russian association[32].

For instance, in April 2014, the Internet Research Agency formed a department that went by various names but was at times referred to as the "translator project." This project focused on the US population and conducted operations on social media platforms such as YouTube, Facebook, Instagram, and Twitter. By approximately July 2016, more than eightyemployees were assigned to the translator project[33].

Subsequently, US officials have uncovered at least 120 fake Russian--backed accounts on Facebook that spread messages seen by 29 million US citizens. These pages include attempts to organise 129 offline, real-world events that were seen by 338,300 people in the United States. Several of these events were attended, but it is unclear how many were indeed attended and how many people participated. As of January 2018, Twitter had identified at least 50,258 Russian bot accounts that posted information related to the US election[34].

On both Facebook and Twitter, Russian accounts allegedly spread messages thought to be disruptive to US civil society or beneficial to Russian goals. This disruption effort included stealing identities and posing as fake US citizens, operating social media pages and other Internet-based media targeted at a US audience and amplifying the views of real but divisive US citizens. Messages sought to exploit and enrage both sides of controversial issues, including gun rights, immigration, LGBT rights and police use of

---

[30] U.S. v. Internet Research Agency, et al, Indictment of 16 February 2018, available at: https://www.justice.gov/file/1035477/download (accessed 5 September 2018), para. 2.

[31] Ibidem, para. 10.

[32] Ibidem, para. 6.

[33] Ibidem, para. 10(d).

[34] Russian Meddling in Elections and referenda in the Alliance, *supra* note, para. 23.

force. They also sought to directly influence the outcome of the 2016 US presidential election. For example, Russian actors sought to undermine Mrs Clinton's candidacy by encouraging minority groups to not vote, supporting her primary opponent and spreading allegations of voter fraud by the US Democratic Party. This "firehose of falsehood," as RAND Corporation researchers describe it, produced high volumes of misinformation over many different channels to demoralise and divide the public[35].

2. Principle of non-intervention in contemporary international law

One of the earliest iterations of the concept of non-intervention was introduced in 1758 by the Swiss philosopher and legal scholar Emer de Vattel. He wrote that "all these affairs being solely a national concern, no foreign power has a right to interfere in them," and "[i]f any intrude into the domestic concerns of another nation . . . they do it an injury."[36]

Almost forty years later, Immanuel Kant, in his essay Perpetual Peace, addressed how governments could achieve and maintain peace while avoiding war. Kant provided that "[n]o state shall by force interfere with the constitution or government of another state."[37]

In 1919, the Covenant of the League of Nations provided one of the earliest codifications of the non-intervention principle. Article 15(8) of the Covenant required that if a "dispute between the parties (...) is found by the [League's] Council to arise out of a matter which (...) s solely within the domestic jurisdiction of [one] party, the Council (...) shall make no recommendation as to its settlement."[38]

In 1933, one of the fundamental instruments of modern international law, the Montevideo Convention, recognized non-intervention as wrongful and provided that "[n]o state has the right to intervene in the internal or external affairs of another."[39]

Since then, the most comprehensive adoption of non-intervention has been recognized by the United Nations Charter, and reflected in numerous United Nations (UN) declarations and reports.

---

[35] Ibidem, para. 24.

[36] Kilovaty, 'Doxfare', *supra* note , 162 (quoting E. de Vattel, *The Law of Nations, Or, Principles of the Law of Nature, Applied to the Conduct and Affairs of Nations and Sovereigns, with Three Early Essays on the Origin and Nature of Natural Law and on Luxury (Indianapolis: Liberty Fund, 2008 (1797), p. 96).*

[37] Ibid. (quoting I. Kant, *Perpetual Peace: A Philosophical Sketch*, 1795, available at: https://www.mtholyoke.edu/acad/intrel/kant/kant1.htm (accessed 28 August 2018), Section I, para. 5).

[38] Covenant of the League of Nations, 28 June 1919, 34 LNTS, Art. 15(8).

[39] Convention on Rights and Duties of States, 26 December 1933, 165 LNTS 19, Art. 8.

A substantial portion of Article 2 of the UN Charter is dedicated to provisions that internalize the principles of sovereignty and non-intervention, though non-intervention is not explicitly mentioned[40].

Article 2(1) acknowledges that the UN is founded on "the principle of the sovereign equality of all its Members",[41] and Article 2(7) clarifies that the Charter does not authorize the UN to "intervene in matters which are essentially within the domestic jurisdiction of any state."[42]

Article 2(4) prohibits what could be described as a "particularly obvious example" of intervention:[43] "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[44]

The UN General Assembly further attempted to establish guiding rules on non-intervention in its Declaration on Friendly Relations, which provides that "[n]o 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"[45] and that "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."[46]

The 1970 Declaration provides a few concrete examples of intervention, including the organization and encouragement of irregular armed forces and assisting or instigating acts of civil strife or terrorism.

"No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State."[47]

---

[40] Gill, 'Non-Intervention in the Cyber Context', *supra* note, 219.

[41] Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945, 1 UNTS 16, Art. 2(1).

[42] Ibidem, Art. 2(7).

[43] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America) (Merits), Judgment of 27 June 1986 (Merits), ICJ Rep 1986, 14, para. 205.

[44] UN Charter, *supra* note, Art. 2(4).

[45] GA 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, 24 October 1970, Annex, Principle 3.

[46] Ibidem.

[47] Ibidem.

Most importantly, however, the Declaration on Principles of International Law proclaims that "[e]very State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State"[48].

The preceding General Assembly Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty contains similar language[49].

Although General Assembly resolutions rarely have legally binding force,[50] the International Court of Justice (ICJ) held these particular declara-

[48] Ibidem.

[49] GA Res 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, 21 December 1965, Preamble ("Reaffirming the principle of non-intervention, proclaimed in the charters of the Organization of American States, the League of Arab States and the Organization of African Unity and affirmed at the conferences held at Montevideo, Buenos Aires, Chapultepec and Bogotá, as well as in the decisions of the Asian-African Conference at Bandung, the First Conference of Heads of State or Government of Non-Aligned Countries at Belgrade, in the Programme for Peace and International Cooperation adopted at the end of the Second Conference of Heads of State or Government of NonAligned Countries at Cairo, and in the declaration on subversion adopted at Accra by the Heads of State and Government of the African States"); *ibid*. ("Recognizing that full observance of the principle of the non-intervention of States in the internal and external affairs of other States is essential to the fulfilment of the purposes and principles of the United Nations"); *ibid*. ("Considering that armed intervention is synonymous with aggression"); *ibid*. ("Considering further that direct intervention, subversion and all forms of indirect intervention are contrary to these principles and, consequently, constitute a violation of the Charter of the United Nations"); *ibid*., para. 1 ("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 condemned"); *ibid*., para. 2 ("No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind"); *ibid*., para. 4 ("The strict observance of these obligations is an essential condition to ensure that nations live together in peace with one another, since the practice of any form of intervention not only violates the spirit and letter of the Charter of the United Nations but also leads to the creation of situations which threaten international peace and security."). See also GA Res. 36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, 9 December 1981 (it sets out framework which , while not declaratory of customary international law, is detailed and specific about the parameters of permissible state actions, with Member States agreeing to: refrain from threaten or use force to disrupt the political, social or economic order of other States; refrain from armed intervention, subversion, military occupation or any act of military, political or economic interference; refrain from any action or attempt to destabilize the political system; refrain from the promotion, encouragement or support, direct or indirect, of any action which seeks to disrupt the unity or undermine or subvert the political order of other States; abstain from any defamatory campaign, vilification or hostile propaganda; abstain from multilateral or unilateral economic reprisal or blockade and to prevent the use of transnational and multinational as instruments of political pressure or coercion; refrain from the exploitation and the distortion of human rights issues as a means of interference). See also D. Raynova, 'Towards a Common Understanding of the NonIntervention Principle', European Leadership Network, October 2017, available at: https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/170929-ELN-Workshop-Report-Non-Intervention.pdf (accessed 30 August 2018), 3.

[50] Kilovaty, 'Doxfare', *supra* note, 163–164.

tions to reflect customary international law. The 1986 *Nicaragua* judgment dismissed both the non-binding nature of General Assembly resolutions, as well as State declarations made at the adoption of the Declaration on Inadmissibility of Intervention, as limitations on the support offered by these provisions to the customary or binding nature of the principle. The Court noted that while upon adoption the United States had indicated 1965 the Declaration on Inadmissibility of Intervention constituted "only a statement of political intention and not a formulation of law",[51] the US statement did not constitute a limit on the Declaration's legal force. The ICJ insisted that the Declaration restated principles committed to without reservation by the US and other States in previous resolutions.[52]The prevalence of non-intervention provisions in other international instruments, such as the Montevideo Convention and the Helsinki Final Act,[53] also influenced the Court's conclusion with respect to the "customary status of the principle which has universal application"[54].

Support for the principle is not limited to the work of the ICJ. The International Law Commission's Declaration on the Rights and Duties of States, provides similar support for the customary status of non-intervention. Article 3 of the Declaration states, "Every State has the duty to refrain from intervention in the internal or external affairs of any other State."[55] The 1949 Declaration is still in the drafting process. Delay appears to have been attributable to a deficit of attention,[56] however, rather than to substantive objections to the Declaration or to Article 3 specifically. As noted above, later meetings of the General Assembly adopted provisions that included the ILC's Article 3 expression of the principle of non-intervention[57].

---

[51] *Nicaragua* case (Merits), *supra* note, para. 203.

[52] Ibidem, ("However, the essentials of resolution 2131 (XX) are repeated in the Declaration approved by resolution 2625 (XXV), which set out principles which the General Assembly declared to be "basic principles" of international law, and on the adoption of which no analogous statement was made by the United States representative.").

[53] Final Act of the Conference on Security and Cooperation in Europe, 1 August 1975, 14 ILM (International Law Materials) 129, Principle VI. The Helsinki Final Act which, while not a multilateral convention in the legal sense, is a politically binding agreement between the Member States of the OSCE. See Gill, 'Non-Intervention in the Cyber Context', *supra* note, 220.

[54] Ibidem, para. 204.

[55] GA Res. 375 (IV) of 6 December 1949, Annex, Art. 3. See also Kilovaty, 'Doxfare', *supra* note, 164.

[56] GA Res. 596 (VI) of 7 December 1951. The General Assembly postponed consideration of the Draft Declaration "until a sufficient number of States have transmitted their comments and suggestions, and in any case to undertake consideration as soon as a majority of the Member States have transmitted such replies." *I*bid.

[57] S. Watts, 'Low-intensity Cyber Operations and the Principle of Non-intervention', in: J. D. Ohlin, K. Govern and C. O. Finkelstein (eds.), *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford: Oxford University Press, 2015) 249–269, 252.

Last but not least, States also regularly express or resort to the principle of non-intervention in legal statements, briefs and memorials to international tribunals[58].

International publicists also have long identified the principle of non-intervention as an essential aspect of the principles of sovereignty and equality among States[59].

3. Alleged interference in 2016 US election under principle of non-intervention

For starters, the principle of non-intervention applies to cyberspace and information technologies and, as such, it was incorporated into the rules of responsible behavior in cyberspace by UN Group of Governmental Experts. The 2015 Report provides that "it is of central importance" that "in their use of [information and communication technologies], States must observe (...) non-intervention in the internal affairs of other States"[60].

Russia, China, and four other States have gone further by drafting and signing an additional non-binding "international code of conduct for information security"[61].

---

[58] Ibid., 250–251 (quoting Briefing remarks of Secretary of State Clinton during the 18 August 2009 meeting with Colombian Foreign Minister Jaime Bermúdez (explaining Defense Cooperation Agreement compliance with "the principle of non-intervention"); the 1996 Statement of Defense of the United States before Iran-United States Claims Tribunal (Claim No. A/30) (quoting reference to the principle of non-interference in bilateral agreement and defending against alleged violation of general principle of noninterference); para. 1 of the 11 December 1994 First Summit of the Americas Miami Plan of Action (quoting Organization of American States members' commitment to the principle of non-intervention – "among its essential purposes is to promote and consolidate representative democracy, with due respect to the principle of non-intervention"); Remarks of the President of the United States, Gerald Ford, in Helsinki on 1 August 1975 (affirming inclusion of principle of non-intervention in Helsinki Final Act)).

[59] Ibidem, 251 (quoting J. Crawford, *Brownlie's Principles of Public International Law* (Oxford: Oxford University Press, 2012), p. 447; M. N. Shaw, *International Law* (Cambridge: Cambridge University Press, 2014), p. 719; L. Oppenheim, *International Law* (London: Longmans, Green and Company, 1912), vol. I, p. 188; R. J. Vincent, *Nonintervention and International Order* (Princeton: Princeton University Press, 1974), p. 310; J. L. Brierly, *The Law of Nations* (Oxford: Oxford University Press, 1955), p. 308; G. G. Wilson, *Handbook on International Law* (St. Paul: West Publishing Company, 1939), pp. 58–59; E. D. Dickinson, *The Equality of States in International Law* (Cambridge, MA: Harvard University Press, 1920), p. 260).

[60] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174, 22 July 2015, available at: https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf (accessed 20 August 2018), para. 26. See also *ibid*., para. 28 (b) ("*In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States.")*.

[61] International code of conduct for information security, UN Doc A/69/723, 13 January 2015, available at: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf (accessed 20 August 2018), Annex.

Intervention was not mentioned in the code, but these States pledged "not to use information (...) to interfere in the affairs of other States or with the aim of undermining [their] political, economic, and social stability"[62].

Finally, the most comprehensive analysis of how existing international law applies to cyber operations, authored by nineteen international law experts, states clearly that "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State"[63].

The rule of non-intervention is a natural derivative of the concept of sovereignty; to the extent that a State enjoys exclusive sovereign rights, other States necessarily shoulder a duty to respect them[64].

The ICJ confirmed the prohibition in its *Nicaragua* judgment, where it observed, "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"[65].

There are two conditions precedent to finding a violation of the prohibition. First, the prohibition only applies to matters that fall within another State's *domaine réservé*.[66] As noted in the 1986 *Nicaragua* judgment, "[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"[67].

These are matters that international law leaves to the sole discretion of the State concerned,[68] such as the "choice of a political, economic, social and cultural system, and the formulation of foreign policy"[69]. J. Ohlin observes that the notion of *domaine réservé* would seem to be "constitutive of the descriptive and normative uses of the phrase "sovereignty", in the sense that being a sovereign State naturally entails the power to act as the sovereign. This is the enduring notion of sovereign prerogative"[70].

---

[62] Ibidem, para. 2(3).

[63] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge/New York: Cambridge University Press, 2017), p. 312.

[64] M. N. Schmitt, 'Grey Zones in the International Law of Cyberspace', (2017) 42(2) Yale JIL (Yale Journal of International Law) 1–21, 7. See also R. Jennings and A. Watts, *Oppenheim's International Law* (London/New York: Longman, 1996), p. 428 (describing the prohibition of intervention as "the corollary of every state's right to sovereignty, territorial integrity and political independence.").

[65] *Nicaragua* case (Merits), *supra* note, para. 202.

[66] Schmitt, 'Grey Zones in the International Law of Cyberspace', *supra* note, 7.

[67] *Nicaragua* case (Merits), *supra* note, para. 205.

[68] Schmitt, 'Grey Zones in the International Law of Cyberspace', *supra* note, 7.

[69] 1970 Declaration on Principles of International Law Concerning Friendly Relations, *supra* note, Principle 3.

[70] J. D. Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', (2017) 95 Texas L Rev (Texas Law Review) 1579–1598, 1587.

At the same time he notes that "the concept has little internally generated content. It has to be spelled out with reference to theories and concepts that are external to the notion of sovereignty. The notion of sovereign prerogative has limits, and almost every international lawyer would agree with this. The question is where to locate the limit-which domains or activities should be off-limits because they fall within a State's domaine reserved and which domains are subject to foreign action"[71].

To illustrate, elections fall within the *domaine réservé*, such that using cyber means to frustrate them would raise issues of intervention. By contrast, purely commercial activities typically do not. Therefore, a State's cyber operations that are intended to afford business advantages to its national companies would not amount to intervention. Between these extremes, the scope of *domaine réservé* is indistinct. For instance, States generally enjoy an exclusive right to regulate online communication in the exercise of its sovereignty. Yet, the point at which international human rights law, such as the rights to freedom of expression or privacy,[72] takes domestic regulation beyond the confines of the *domaine réservé* remains unsettled[73].

Second, the *Tallinn Manual 2.0*argues that an intervention against a State's choice of political structure would count as an infringement against its *domaine réservé*, but only in the case where the intervention is accompanied by some degree of coercion[74].

The term coercion "refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way"[75].

Accordingly, the drafters of the *Tallinn Manual 2.0* do not view the spreading of propaganda as, by itself, indicative of an illegal intervention against another State's *domaine réservé*:"[C]oercion must be distinguished from persuasion, criticism, public diplomacy, propaganda, retribution, mere maliciousness, and the like in the sense that, unlike coercion, such activities merely involve either influencing (as distinct from factually compelling) the volun-

---

[71] Ibidem, 1587–1588.

[72] GA Res. 217 (III) A, Universal Declaration of Human Rights, 10 December 1948, Arts. 12, 19; International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171, Arts. 17, 19(2).

[73] Schmitt, 'Grey Zones in the International Law of Cyberspace', *supra* note, 7.

[74] *Tallinn Manual 2.0*, *supra* note, p. 317.

[75] Ibidem, See also M. N. Schmitt, "Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', (2018) 19(1) Chicago JIL (Chicago Journal of International Law) 30–67, 51 (defining coercion as "coercive action is intended to cause the State to do something, such as take a decision that it would otherwise not take, or not to engage in an activity in which it would otherwise engage." Thus, coercion can be said to "subordinate the sovereign will of the target State".").

tary actions of the target State or seek no action on the part of the target State at all"[76].

In other words, blocking voting by cyber means, such as by disabling election machinery or by conducting a distributed denial of service attack, would likewise be coercive. In both of these situations, the result of the election, which is the expression of the freedom of choice of the electorate, is being manipulated against the will of the electorate. Nevertheless, those actions described as lawful in the context of sovereignty violations, like espionage, slanted media reporting by Russian controlled media, and the purchase of advertising to sway the electorate in favor of a particular candidate, are similarly not coercive and do not qualify as a prohibited intervention[77].

Schmitt's conclusion is supported by State practice. the United States and other countries have dropped leaflets on the territory of another State in order to convince a foreign population to pressure its leaders into a course of action. The *Voice of America* broadcasts across the globe in order to provide information to foreign audiences. The government of South Korea places loudspeakers near the border with North Korea in order to disseminate news and information that might not otherwise reach its epistemically isolated population. No one denies that Putin would have been permitted to speak publicly on Russia Today, the decidedly proPutin State television network, and declare his support for Trump and urge all Americans to vote for him. This right to engage in the political process is hardly a violation of America's *domaine réservé*[78].

Schmitt himself offers, however, a different perspective on permissibility of the 2016 Russian interference under prohibition of intervention in international law.

The covert nature of the troll operation deprived the American electorate of its freedom of choice by creating a situation in which it could not fairly evaluate the information it was being provided. As the voters were unaware that they were being manipulated by a foreign power, their decision making, and thus their ability to control their governance, was weakened and distorted. The deceptive nature of the trolling is what distinguishes it from a mere influence operation. And it can be argued that the hacking and release tainted the electoral process by introducing information that, albeit genuine, was acquired by means that are expressly prohibited under US domestic law, as well as the law of most other States—namely, the unlawful penetra-

---

[76] *Tallinn Manual 2.0*, *supra* note, pp. 318–319.

[77] Schmitt, 'Cyber Election Meddling in the Grey Zones of International Law', *supra* note, 50.

[78] Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *supra* note, 1588.

tion and exfiltration of private data. In this sense, the electorate's freedom of choice was being thwarted[79].

Moreover, it remains unresolved whether coercion requires a direct causal nexus between the act in question and the coercive effect, as in the case of changing election results. As *Tallinn Manual 2.0* states, "It is certainly the case that coercion need not be direct and may come in an indirect form: Coercion sufficient to support a finding of unlawful intervention may take either a direct or indirect form. In its findings of fact, the International Court of Justice in the Nicaragua judgment determined that the United States had supplied assistance to rebels, including "training, arming, equipping ... [rebel] military and paramilitary actions in and against Nicaragua." The court held that the principle of non-intervention "forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States"[80].

This is an essential distinction because the aforementioned Russian activities were indirect in the sense that, while they may have affected the voters' choice of candidates, or even their decision to vote at all, the operations did not in themselves alter the result. If indirect causation satisfies the causal facet of coercion, the fact that intervention need not be directed against governmental election infrastructure is of particular importance, for it means that cyber operations directed against a political party could qualify. An example would be a denial of service attack against the party's website, blog, email or other forms of online campaigning at a critical juncture in the election. A cyber operation that generated false messages purportedly from the party and attempted to sway votes or alter the party's actual messaging in a significant way also would qualify[81].

Last but not least, President Trump has repeatedly suggested that any election meddling that might have occurred did not affect the outcome. However, whether this is true as a matter of fact is irrelevant as a matter of law. The internationally wrongful act of prohibited intervention does not require that the cyber operations in question be successful. It only requires that they be intended to have a coercive effect with respect to a *domaine réservé*, in this case elections[82].

Other scholars have also concluded that the Russian hacking included some coercive element, implicitly rejecting the requirement of an impermissible consequence. For example, S. Barela states that, "coercion can be un-

---

[79] Schmitt, 'Cyber Election Meddling in the Grey Zones of International Law', *supra* note, 51.

[80] *Tallinn Manual 2.0*, *supra* note, pp. 319–320.

[81] Schmitt, 'Cyber Election Meddling in the Grey Zones of International Law', *supra* note, 51–52.

[82] Ibidem, 52.

derstood as more than simply forcing an electoral outcome. The significance and expanse, both in scale and reach, of the interests targeted are relevant. Whether the Russian meddling was meant to achieve a particular result in the election (wishing to aid one candidate over another), there were also more important-even if less tangible-matters at stake"[83].

Ohlin quotes M. McDougal and F. Feliciano to suggest that one possibility for defining coercion is simply the scale and effect of the overall intervention, which in this case was quite substantial[84].

Conclusions

Did Russian interference in the 2016 US presidential election violate prohibition of non-intervention under treaty and customary law?

Concerning the factual background of the analysis, activities discussed above were massive including cyberespionage against US political organizations, public disclosures of data obtained through covert intelligence activities, overt propaganda by state-funded media, cyberintrusions into US state and local electoral boards and "fake news" influence efforts in social media. Their legal assessment from the perspective of unlawful intervention into the internal affairs of another State gives no clear answer.

Two elements must be satisfied before a cyber operation qualifies as wrongful intervention. The operation must affect a State's domaine réservé and it must be coercive.81 Absent one of these elements, the operation may constitute interference, but it will not rise to the level of unlawful intervention.

Undeniably, the holding of a federal election is an inherently governmental function in a liberal democracy. So, in theory, the disruption of an election should count as the usurpation of an inherently governmental function.[85]Indeed, the drafters of the *Tallinn Manual 2.0*listed a number of governmental functions, including "changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the

---

[83] S. J. Barela, 'Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion', Just Security, 12 January 2017, available at: https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/ (accessed 20 June 2018).

[84] Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *supra* note , 1593 (quoting M. S. McDougal and F. P. Feliciano, 'International Coercion and World Public Order: The General Principles of the Law of War', (1958) 67 Yale LJ (Yale Law Journal) 771–845, 782 (noting that coercion is defined by three dimensions of consequentiality, including "the importance and number of values affected, the extent to which such values are affected and the number of participants whose values are so affected.").

[85] Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *supra* note, 1593–1594.

collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities"[86].

In the 2016 election, however, the Russian government allegedly released private information to the public, rather than "changing or deleting" it.[87]The interference constituted the "influence campaign",[88] including disclosure of private information and possibly distribution of fake news stories, falling under the umbrella of propaganda and violations of the right to privacy. Moreover, the Tallinn Manual does not further define what constitutes the "conduct of elections".

Everyone agrees that had the Russian government tampered with the ballot boxes, or with electronic voting, this would count as a violation of international law, because the counting of votes during an election is a paradigmatically "governmental function", which in that case would be "usurped" by Russia. Votes should be tabulated, counted, and reported by the government officials administering the election, and any interference with that process sounds like a usurpation of an inherently governmental function. At this moment in time, however, there is no publicly available evidence that the Russian cyber interference included tampering with the vote-tabulation process.

As Ohlin concludes: "We are left then with an overall impression of illegal conduct, but without a clear and unambiguous doctrinal route towards that conclusion"[89].

With respect to the second element, coercion can be said to "subordinate the sovereign will of the target State", in the case of elections this might manifest in the election of a candidate who otherwise would not win, the weakening of a successful candidate's political base, or the strengthening of an unsuccessful candidate's base in anticipation of future elections.[90] Schmitt admits, however, that the will of the people cannot be determined with any degree of certainty before an election.[91] The separate problem con-

---

[86] *Tallinn Manual 2.0*, *supra* note, p. 22.

[87] Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *supra* note, 1594.

[88] 'Assessing Russian Activities and Intentions in Recent US Elections', *supra* note , 1 ("We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. (...) We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.).

[89] Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *supra* note, 1594.

[90] Schmitt, 'Cyber Election Meddling in the Grey Zones of International Law', *supra* note, 51.

[91] Ibidem, 55.

cerning illegality of Russian measures in the context of legal finding of coercion refers to identification of some individual or group as the target of the coercion. Was it the American voters? Were they coerced into voting for Trump and not for Clinton? If so, what were the threatened consequences? One might argue that the Russian intervention came with an implied threat to withhold benefits if Hillary Clinton were elected and that Russia would act in a more cooperative manner towards the United States if Trump were elected, perhaps in exchange for reciprocal considerations from a new Trump Administration. Or perhaps one might argue that the hacking came with the threat of future illegal behavior on the part of the Russian government: either more instances of hacking, or more daringly, increased military aggression in places like Crimea or eastern Ukraine. Or, one might assume that the object of the coercion was actually Hillary Clinton. In that regard, perhaps the point was that Clinton was implicitly informed that she should adopt a more conciliatory attitude toward Russia (and drop any attempts to pursue regime change in Russia or oust Putin), and that if she did not comply, the hacking of DNC e-mails would be the threatened consequence[92].

Summing up, while there is no disagreement over whether the prohibition comprises a primary rule of international law, its applicability in the context of the 2016 Russian election meddling, is characterized by substantial uncertainty. As there are clear-cut cases that either do or do not breach the meddling State's obligations concerning prohibition of intervention, Russian actions have successfully exploited a significant grey zone lies between the easy cases, particularly with respect to indirect coercion. While the Russian hacking was certainly corrosive, it is genuinely unclear whether it should count as coercive[93].

Treaties and legal documents

Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945, 1 UNTS 16, Art. 2(1).

International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.

Final Act of the Conference on Security and Cooperation in Europe, 1 August 1975, 14 ILM (International Law Materials) 129.

GA Res. 217 (III) A, Universal Declaration of Human Rights, 10 December 1948.

GA Res. 375 (IV) of 6 December 1949.

[92] Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *supra* note, 1592.

[93] Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *supra* note, 1593; Schmitt, 'Cyber Election Meddling in the Grey Zones of International Law', *supra* note , 52–53.

GA Res. 596 (VI) of 7 December 1951.
GA Res 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, 21 December 1965.
GA 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, 24 October 1970.
Case concerning military and paramilitary activities in and against Nicaragua (*Nicaragua v. United States of America*) (Merits), Judgment of 27 June 1986 (Merits), ICJ Rep 1986, 14.

Literature

Egan B. J., 'Remarks on *International Law and Stability in Cyberspace*, Berkeley Law School, (*November 10, 2016)*', (2017) 35(1) Berkeley JIL (Berkeley Journal of International Law) 169–180.
Gill T. D., 'Non-Intervention in the Cyber Context', in: K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013) 217–238.
Kilovaty I., 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information', (2018) 9 Harvard NSJ (Harvard National Security Journal) 146–179.
Ohlin J. D., 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', (2017) 95 Texas L Rev (Texas Law Review) 1579–1598.
Raynova D., 'Towards a Common Understanding of the NonIntervention Principle', European Leadership Network, October 2017, available at: https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/170929-ELN-Workshop-Report--Non-Intervention.pdf (accessed 30 August 2018).
Schmitt M. N., 'Grey Zones in the International Law of Cyberspace', (2017) 42(2) Yale JIL (Yale Journal of International Law) 1–21.
Schmitt M. N., "Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', (2018) 19(1) Chicago JIL (Chicago Journal of International Law) 30–67.
Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (Cambridge/New York: Cambridge University Press, 2017).
Van De Velde J., 'The law of Cyber Interference in Elections', SSRN, 15 May 2017, available at: https://ssrn.com/abstract=3043828(accessed 3 August 2018).
Watts S., 'Low-intensity Cyber Operations and the Principle of Non-intervention', in: J. D. Ohlin, K. Govern and C. O. Finkelstein (eds.), *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford: Oxford University Press, 2015) 249–269.

Streszczenie

Domniemana rosyjska ingerencja w wybory prezydenckie w USA w 2016 r. w świetle zasady nieinterwencji

Słowa kluczowe: zakaz interwencji w sprawy wewnętrzne państw, interwencja w cyberprzestrzeni, ingerencja zewnętrzna w proces wyborczy, wybory prezydenckie w USA w 2016 r.

Opracowanie podejmuje zagadnienie zakazu interwencji w sprawy wewnętrzne innych państw na tle problemu domniemanej rosyjskiej ingerencji w wybory prezydenckie w USA w 2016 r. Analiza stanowi kompendium wiedzy na temat zakresu i metod ingerencji, przygotowane w oparciu o dokumenty wspólnoty wywiadowczej oraz biura prokuratora specjalnego Departamentu Sprawiedliwości USA w okresie od stycznia 2017 do lipca 2018 r. Przedmiotem rozważań jest również zakres i treść zakazu interwencji we współczesnym prawie międzynarodowym. Elementem podsumowującym opracowanie jest ocena legalności zidentyfikowanych metod rosyjskiej ingerencji w amerykańskie wybory prezydenckie z perspektywy prawa międzynarodowego.

Summary

Keywords: prohibition of intervention under contemporary treaty and customary law, intervention in cyberspace, interference in elections, 2016 US presidential election.

Article involves principle of non-intervetion in the context of a alleged Russian alleged Russian interference in the US 58th quadrennial presidential election. Analysis includes review of methods and means of the 2016 cyberintervention, based on a January 2017 assessment of the US intelligence community and 2018 indictments prepared by the Office of Special Counsel. It is followed by examination of legal Nature and scope of the principle of non-intervention under contemporary treaty and customary international law. In the last section conclusions will be drawn in relation to the applicability of the legal framework relating to non-intervention to the alleged Russian interference in the 2016 presidential election.