GRILI WORKING PAPER NO.3

Revue belge de droit international (forthcoming in 2021)

NO INTERFERENCE, NO PROBLEM: VOTER INFLUENCE OPERATIONS AND INTERNATIONAL LAW

December/2020

Luca Ferro
Ghent Rolin-Jaequemyns International Law Institute (GRILI), Ghent University

GHENT UNIVERSITY

Revue belge de droit international (forthcoming in 2021)

NO INTERFERENCE, NO PROBLEM: VOTER INFLUENCE OPERATIONS AND INTERNATIONAL LAW

by Luca Ferro[1]

Abstract

The 2016 US Presidential Election was marred by (cyber-)meddling allegedly directed by Russia and aimed at sowing discord in the political system, boost Donald Trump's election chances, and steal voter data and other sensitive information. Using that alleged Russian involvement in the 2016 election as a case study, this article examines its legality under public international law.

Numerous books, articles and blog posts have since dealt with this issue, focusing on (all or some of) such primary international legal norms as the principle of sovereign equality of States, the principle of non-intervention, the right to self-determination, the duty of due diligence and the human right to privacy. Almost without exception, although expressed with varying degrees of confidence, commentators concluded that one or more of these norms were violated leading up to the 2016 election, resulting in a fragile yet broad academic consensus on the illegality of the Russian operation and, by extension, VIOPS. This article aims to revisit and challenge that consensus.

It starts with an overview of case facts as well as the domestic and international reactions to which they gave rise in Section 2. Section 3 then zooms in on three key (and interrelated) international legal norms: sovereignty, non-intervention and self-determination. It applies these legal standards (as interpreted) to the facts (as assumed). Finally, Section 4 wraps up the legal analysis and concludes.

Keywords

Voter influence operations (VIOPS), international law in cyberspace, the principle of sovereign equality, the principle of non-intervention, the right to self-determination

[1] Postdoctoral researcher, Ghent Rolin-Jaequemyns International Law Institute (GRILI), Ghent University, Belgium. Luca.Ferro@UGent.be.

"We are determined to work collaboratively to reinforce our democracies against illicit and malign behavior and foreign hostile interference".

G7, Australia, Chile, India & South Africa, 26 August 2019

"President Trump told two senior Russian officials in a 2017 Oval Office meeting that he was unconcerned about Moscow's interference in the 2016 U.S. presidential election because the United States did the same in other countries".

The Washington Post, 28 September 2019

We call on the US "[t]o jointly develop and conclude a bilateral intergovernmental agreement on preventing incidents in the information space".

Russian President Vladimir Putin, 25 September 2020

1 Introduction[2]

According to Dov Levin, the United States and the Soviet Union(/Russia) have 'intervened in about one of every nine competitive national-level executive elections' between 1946 and 2000 – with the US' share amounting to 69% of those.[3] Levin's empirical work focused on so-called partisan electoral interventions, including the provision of campaign funds, public and specific promises or threats by official representatives, the sudden provision or withdrawal of foreign aid, and the covert dissemination of scandalous exposés and disinformation on rival

[2] This article has been a long time in the making, with several drafts that have been presented to respondents in various settings. It has benefited tremendously from their comments, and I am therefore grateful to Professors Tom Ruys, Karen Knop, Melissa J. Durkee, Anne Orford, Lori F. Damrosch and, as members of my doctoral examination board, Olivier Corten, Michael Wood, Erika De Wet, An Cliquet and Frank Maes – as well as the two peer reviewers of the *Revue belge de droit international*. Moreover, the article was finished in late October 2020 – so days before the 2020 US election, convincingly won by former Vice-President Joe Biden. In addition, the Oxford Statement on International Law Protections against Foreign Electoral Interference through Digital Means was released days after submitting my article for review, which has been signed by more than 150 renowned public international lawyers, including many of those referred to in this piece (see: <https://elac.web.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through?fbclid=IwAROJH_jh84jA8lfHQ1_dko-W5VZ8tN87l-UsP6XWEduCYRAMNOjeha-poqU>). However, the statement is formulated rather equivocally. For example, it notes that a State must refrain from 'interfering … with electoral processes', 'conducting cyber operations that adversely impact the electorate's ability to participate in electoral processes, to obtain public, accurate and timely information thereon, or that undermine public confidence in the integrity of electoral processes' as well as 'conducting operations that violate the right to privacy, freedom of expression, thought, association and participation in electoral processes'. But it by no means clarifies *when, exactly* a State falls foul of that prohibition, beyond referring to vague 'adverse consequences' such as 'interven[ing] in the conduct of an electoral process' (begging the question) or 'undermin[ing] public confidence in the official results or the process itself' (difficult to operationalize). That is of course the crux of the legal debate, which may explain why so many lawyers are comfortable in signing on even though their work reveals significant differences in approach – see below. And while I agree that the *absence* of interference likely means international law emerges unscathed, it is submitted that its mere *presence* does not necessarily mean the law is violated. Finally, the three quotes with which this article started can be found here: G7, 2019 Biarritz Summit, 'Biarritz Strategy for an Open, Free and Secure Digital Transformation' (26 August 2019) <https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf> para 4; S Darcy et al, 'Trump Told Russian Officials in 2017 He Wasn't Concerned about Moscow's Interference in U.S. Election' *The Washington Post* (28 September 2019) <https://www.washingtonpost.com/national-security/trump-told-russian-officials-in-2017-he-wasnt-concerned-about-moscows-interference-in-us-election/2019/09/27/b20a8bc8-e159-11e9-b199-f638bf2c340f_story.html>; Russia, President of Russia, 'Statement by President of Russia Vladimir Putin on a Comprehensive Program of Measures for Restoring the Russia – US Cooperation in the Filed [sic] of International Information Security' (25 September 2020) <http://en.kremlin.ru/events/president/news/64086>.

[3] D Levin, 'Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset' (2016) 36 Conflict Management and Peace Science 88, 2 and 7.

candidates.[4] At the same time Levin's seminal article was published, in 2016, the US Presidential Election was being targeted by Russian operatives in what has perhaps become the best-known example of the research topic.[5]

Using that alleged Russian involvement in the 2016 election as a case study, this article examines its legality under public international law. For that purpose, it employs the broad concept of 'voter influence operations' (or VIOPS) to generally denote efforts to influence a democratic election abroad that are directed(/sanctioned) by a State.[6] In addition, it relies on the typology used by the *EU vs Disinfo* website – run by the European Union's East Stratcom Task Force – distinguishing four categories of influence operations (information manipulation, cyber disruption, political grooming and extreme intervention) and ten such methods (including disinformation, sentiment amplification, identity falsification, hack-and-leak operations, infrastructure hacks and campaign financing).[7]

Numerous books, articles and blog posts have since dealt with this issue, focusing on (all or some of) such primary international legal norms as the principle of sovereign equality of States, the principle of non-intervention, the right to self-determination, the duty of due diligence and the human right to privacy.[8] Almost without exception, although expressed with varying degrees of confidence, commentators concluded that one or more of these norms were violated leading up to the 2016 election, resulting in a fragile yet broad academic consensus on the illegality of the

---

[4] ibid 4, table I.

[5] See also: D Levin, *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions* (OUP 2020) Chapter 8.

[6] Compare with Levin's definition ((n 3) 3). See also: 'Methods of Foreign Electoral Interference' (*EU vs Disinfo*, 2 April 2019) <https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/>.

[7] 'Methods of Foreign Electoral Interference' (n 6).

[8] D Hollis, 'Russia and the DNC Hack: What Future for a Duty of Non-Intervention' (*Opinio Juris*, 25 July 2016) <http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/>; S Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack' (*Just Security*, 14 October 2016) <https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/>; C Forcese, 'The "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?' (*Just Security*, 16 December 2016) <https://www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/>; H Koh, 'The Trump Administration and International Law' (2017) 56 Washburn Law Journal 413; I Kilovaty, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information' (2018) 9 Harvard National Security Journal 146; R Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace' (2018) 103 CLRev 565; S Barela, 'Zero Shades of Grey: Russian-Ops Violate International Law' (*Just Security*, 29 March 2018) <https://www.justsecurity.org/54340/shades-grey-russian-ops-violate-international-law/>; M Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 ChiJIntlL 30; D Efrony and Y Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 AJIL 583; B Sander, 'Democracy under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019) 18 CJIL 1; N Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' (*EJIL:Talk!*, 26 August 2019) <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/>; H Moynihan, Chatham House, 'The Application of International Law to Cyberattacks: Sovereignty and Non-Intervention' (December 2019) <https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf>; M Helal, 'On Coercion in International Law' (2019) 52 NYUJIntlL&Pol 1; M Milanovic and M Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations during a Pandemic' (2020) Journal of National Security Law & Policy (forthcoming, but available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3612019>); C Keitner, 'Foreign Election Interference and International Law' in D Hollis and J Ohlin (eds), *Election Interference: When Foreign Powers Target Democratic Institutions* (forthcoming, but available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3599586>); H Lahmann, 'Information Operations and the Question of Illegitimate Interference under International Law' (2020) 53 IsLR 189; J Ohlin, *Election Interference: International Law and the Future of Democracy* (CUP 2020). See also the International Cyber Law in Practice: Interactive Toolkit, developed and supported by *inter alia* the International Committee of the Red Cross (ICRC) and NATO Cooperative Cyber Defence Centre of Excellent, at: <https://cyberlaw.ccdcoe.org/wiki/Main_Page> (first general annual update on 2 October 2020). On two primary norms that are not this article's focus, the extraterritorial application of human rights and the due diligence principle in cyberspace, see: M Milanovic, 'Surveillance and Cyber Operations' in M Gibney et al (eds), *Research Handbook on Extraterritorial Human Rights Obligations* (forthcoming, but available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3708440> and K Bannelier, 'Obligations de diligence dans le cyberspace: Qui a peur de la cyber-diligence?' (2017/2) Revue belge de droit international 612 (respectively).

Russian operation and, by extension, VIOPS. This article aims to revisit that consensus. It starts in earnest with an overview of case facts as well as the domestic and international reactions to which they gave rise in Section 2. Section 3 then zooms in on three key (and interrelated) international legal norms: sovereignty, non-intervention and self-determination. It applies these legal standards (as interpreted) to the facts (as assumed). Finally, Section 4 wraps up the legal analysis and concludes.

But before delving into the facts and associated legal intricacies, a number of preliminary comments are in order: First, the legal analysis will assume that the influence operation was in fact directed by Russia to which it can, therefore, be attributed under the Articles on State Responsibility for Internationally Wrongful Acts (ARSIWA).[9] Attribution will, consequently, be taken as a given and receive comparatively little attention.[10] Second, while the article is interspersed with some examples of *domestic* legislation on the involvement of foreign actors during elections, it does not provide a comparative overview of such legislation in different countries. Rather, the focus will (almost) exclusively be on the *international* legal framework and the extent to which it independently prohibits (or is silent on) voter influence operations or VIOPS.

2 Russia and the 2016 US Presidential Election

2.1 Facts

The dust is beginning to settle on Russia's nefarious role in the controversial election of US President Donald Trump on 8 November 2016. Two major, official investigations in the US have now been concluded and published (albeit heavily redacted),[11] while 34 individuals (including 12 officers of the Russian military intelligence service) and three Russian companies have been charged for committing federal crimes under US law in that context.[12]

For the purposes of this article, three specific actions will be scrutinized, taking the allegations made in the reports as fact for argument's sake: the sophisticated social media campaign (with some overflow into 'meatspace'[13]), the

[9] 'Draft Articles on Responsibility of States for Internationally Wrongful Acts: Text' (2001) II(2) YILC 26, arts 4-11.
[10] See, for example: United States, Senate Select Committee on Intelligence, 'Russian Active Measures Campaign and Interference in the 2016 U.S. Election: – Volume V: Counterintelligence Threats and Vulnerabilities' (18 August 2020) <https://www.intelligence.senate.gov/press/senate-intel-releases-volume-5-bipartisan-russia-report>: 'the Russian government engaged in an aggressive, multifaceted effort to influence … the outcome of the 2016 presidential election.'
[11] United States, Department of Justice, Special Counsel's Office, 'Report on the Investigation into Russian Interference in the 2016 Presidential Election' (March 2019) <https://www.justice.gov/storage/report.pdf> (Mueller report); United States, Senate Select Committee on Intelligence, 'Russian Active Measures Campaign and Interference in the 2016 U.S. Election' (2019-2020) <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures> (Senate Intelligence Committee report). The reports largely confirm, and expand on, another that was released two weeks before Trump's inauguration: United States, Office of the Director of National Intelligence, 'Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections' (6 January 2017) <https://www.dni.gov/files/documents/ICA_2017_01.pdf> (ICA report).
[12] United States, Department of Justice, Special Counsel's Office, at: <https://www.justice.gov/sco>. See also: A Prokop, 'All of Robert Mueller's Indictments and Plea Deals in the Russia Investigation' *VOX* (updated on 17 December 2019) <https://www.vox.com/policy-and-politics/2018/2/20/17031772/mueller-indictments-grand-jury>.
[13] The word is patterned after 'cyberspace' and used to denote the 'real' or 'off-line' world, see: <https://www.merriam-webster.com/words-at-play/what-is-meatspace>.

hack-and-leak of private emails and other documents (or 'doxfare'[14]), and the targeting of election infrastructure. As such, the focus will be on two categories of voter influence operations: information manipulation and cyber disruption. Taken together, they include such methods as disinformation, political advertising, sentiment amplification, identity falsification, hack-and-leak operations, reconnaissance hacking and infrastructure attacks.[15]

2.1.1 The Internet Research Agency's use of social media[16]

The Internet Research Agency (IRA) is an organization based in St. Petersburg (Russia) and funded by Russian national Yevgeny Prigozhin through several of his companies. Prigozhin is colloquially known as 'Putin's Cook' for securing significant catering contracts for state banquets and most of the Russian military, and his close ties to Russian President Vladimir Putin.[17] Under Prighozin's tutelage, the IRA was accused of creating and managing multiple social media accounts on Facebook, Twitter, YouTube, Instagram and Tumblr during the 2016 election, reaching approximately 126 million Americans through Facebook alone.[18] Moreover, several IRA-tweets were cited or retweeted by high-profile individuals in the Trump campaign, including his sons and campaign manager.[19]

Generally, the IRA's social media campaign followed a specific *modus operandi*: it created fake accounts impersonating US individuals or falsely claiming affiliation with US political and grassroots organizations. These accounts were then boosted through advertisements (on Facebook) or a network of automated bots (on Twitter). Its messages were designed to amplify divisive political and social issues – such as race, immigration and Second Amendment rights – and took sides in the election process by hurting Democratic Presidential Nominee Hillary Clinton and helping her Republican adversary Donald Trump. The campaign's sophistication appears to have been improved through an intelligence-gathering mission on US soil by two IRA-employees beginning in June 2014. Finally, the IRA instigated unwitting US citizens into organizing and promoting dozens of political rallies, and the IRA-organization 'Black Fist' even hired a self-defence instructor in New York to 'teach African-Americans to protect themselves when contacted by law enforcement'.[20]

---

[14] Ido Kilovaty defines the term as 'state-sponsored intrusions into foreign computer systems and networks to collect bulk, non-public data that are then leaked for public consumption', see: Kilovaty (n 8) 152-3. It is a play on the words doxing (publishing private information as a form of punishment or revenge) and lawfare (using the law instead of military methods to achieve operational objectives).

[15] 'Methods of Foreign Electoral Interference' (n 6).

[16] While much of the factual information for this section comes from the Mueller report, volume I (n 11), more information can be found in the specific indictment (on which it relied): United States, District Court for the District of Columbia, *USA v Internet Research Agency LLC et al*, Case 1:18-cr-00032-DLF, 16 February 2018.

[17] Mueller report, volume I (n 11) 16-17; Senate Intelligence Committee report, volume II (n 11) 23-4.

[18] Mueller report, volume I (n 11) 15 and 26.

[19] ibid 33-4.

[20] ibid 14ff, 21 and 29-32.

2.1.2 *Doxfare by the Main Directorate of the General Staff of the Russian Army (GRU)*[21]

At the same time as, but distinct from, the IRA social media campaign, units of the GRU launched a large-scale cyber-operation against computer networks and personal email accounts of individuals linked to the Clinton campaign, the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). The GRU successfully implanted specialized malicious software (malware) and conducted a large-scale spear phishing campaign, resulting in the exfiltration of hundreds of thousands of documents, including private emails, internal strategy documents, fundraising data and opposition research.[22] Ultimately, the documents were released through at least two fictitious online personas created by the GRU, DCLeaks and Guccifer 2.0, and the organization WikiLeaks (run by Australian national Julian Assange).[23]

Again, the doxing operation was aimed primarily at damaging Hillary Clinton by, for example, publishing her private paid speeches to Wall Street executives and evidencing the pervasive anti-Bernie Sanders – her opponent in the primary – sentiment in the DNC.[24] At the same time, the campaign greatly benefited Donald Trump. For example, a batch of politically explosive emails from Clinton campaign chairman John Podesta was released within an hour of the US intelligence agency's official accusation against Russia for email hack-and-release operations and the publication of the infamous Access Hollywood tape, capturing Donald Trump speaking in lewd terms about women.[25]

2.1.3 *Russian infiltration of the US election infrastructure*

Finally, unidentified Russian operatives were thought responsible for the reconnaissance hacking of election-related infrastructure, likely affecting all 50 US states, including 'state boards of elections, secretaries of state, county governments, private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations'.[26] That activity was helpfully explained as

---

[21] See also (n 16) and: United States, District Court for the District of Columbia, *USA v. Netyksho et al*, Case 1:18-cr-00215-ABJ, 13 July 2018.

[22] Spear phishing emails were used to trick the recipient into downloading customized malware (e.g., tools to harvest credentials, prepare material for exfiltration and take screenshots) was implanted in DCCC and DNC networks. In addition, such emails were also designed to appear as originating from a trusted source to solicit information (e.g., passwords) to enable the sender to gain access to an account or network. See: Mueller report, volume I (n 11) 36-40.

[23] ibid 41-9. See also: Senate Intelligence Committee report, volume II (n 11) 68.

[24] A Yuhas, 'Hillary Clinton Campaign Blames Leaked DNC Emails about Sanders on Russia' *The Guardian* (24 July 2019) <https://www.theguardian.com/us-news/2016/jul/24/clinton-campaign-blames-russia-wikileaks-sanders-dnc-emails>; A Chozick et al, 'Leaked Speech Excerpts Show a Hillary Clinton at Ease with Wall Street' *The New York Times* (7 October 2016) <https://www.nytimes.com/2016/10/10/us/politics/hillary-clinton-emails-wikileaks.html>. See also: Mueller report, volume I (n 11) 44-5 on WikiLeaks' antipathy towards Clinton.

[25] M Cohen, 'Access Hollywood, Russian Hacking and the Podesta Emails: One Year Later' *CNN* (7 October 2017) <https://edition.cnn.com/2017/10/07/politics/one-year-access-hollywood-russia-podesta-email/index.html>; United States, Department of Homeland Security, 'Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security' (7 October 2016) <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>.

[26] Mueller report, volume I (n 11) 50; Senate Intelligence Committee report, volume I (n 11) 10-2.

> simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home. A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in … [however] a small number of the networks were successfully exploited. They made it through the door.[27]

The last comment refers to the hackers' success in accessing the election infrastructure systems in (at least) two states and extracting large amounts of voter data (e.g., the voter registration information of 14 million citizens in the state of Illinois).[28]

In the end, the US Senate Select Committee on Intelligence concluded that there were 'no indications that votes were changed, vote-tallying systems were manipulated, or that any voter registration data was altered or deleted', even if the Committee humbly admitted that its insight was 'limited'. It also remained in the dark regarding Russia's intentions, but thought it most likely they were aimed at 'undermining the integrity of elections and American confidence in democracy'.[29]

2.2 Reactions by the protagonists, third States and international organizations

Then US President Barack Obama privately warned Putin to 'cut it out' in September 2016 (i.e., two months *before* the election), threatening 'serious consequences' if he did not.[30] However, the first official reaction came only *after* the election, when his administration announced sanctions against entities and individuals involved in 'efforts to harm U.S. interests in violation of established international norms of behavior'.[31] Unsurprisingly, Clinton described the operation more strongly as 'cyberwarfare': 'it's not tanks and planes and ships, but it is a form of war'.[32] Conversely, Trump never admitted Russia was involved, disputing the assessment of his intelligence agencies after his inauguration: 'My people came to me … they said they think it's Russia. I have President Putin; he just said it's not Russia.'[33] Russia also vociferously denied any involvement.[34] In one hard-hitting interview that discussed the IRA-social media campaign at length after the indictment was issued, Putin claimed he 'simply [did] not know anything

---

[27] Senate Intelligence Committee report, volume I (n 11) 11.
[28] ibid 22.
[29] ibid 35ff, including possible examples of how that objective could have been reached.
[30] L Nelson, 'Obama Says He Told Putin to "Cut It Out" on Russia Hacking' *Politico* (16 December 2016) <https://www.politico.com/story/2016/12/obama-putin-232754>.
[31] United States, Office of the Press Secretary, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment' (29 December 2016) <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity>. For the latest, and an overview, see: United States, Department of the Treasury, 'Treasury Sanctions Russia-Linked Election Interference Actors' (10 September 2020) <https://home.treasury.gov/news/press-releases/sm1118>.
[32] A Hoffman, 'Hillary Clinton: Russia's 2016 Election Meddling Is a "Form of War"' *Time* (2 November 2017) <https://time.com/5007112/hillary-clinton-trump-russia-daily-show/> (video clip, starting at 1'20").
[33] United States, The White House, 'Remarks by President Trump and President Putin of the Russian Federation in Joint Press Conference' (16 July 2018) <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-putin-russian-federation-joint-press-conference/>.
[34] See, e.g., official reactions by the Russian Ministry of Foreign Affairs to the ICA report (n 11) and *USA v. Netyksho et al* indictment (n 21): 'Briefing' (18 May 2017) <http://www.mid.ru/en/press_service/spokesman/briefings/-/asset_publisher/D2wHaWMCU60d/content/id/2761759> ('a school essay with not a single true fact'); 'Comment by the Information and Press Department regarding the latest US Anti-Russia Allegations' (13 July 2018) <http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3294871> ('a shameful and disgraceful act') (respectively).

about it' and that at 'the level of the Russian Government and … President, there has never been any interference in the internal political processes in the [US]'.[35] However, he did acknowledge that Russian citizens might have been involved: 'Well, all right, Russians, but they were not state officials. Well, Russians, and so what?'. He repeatedly expressed the view that nothing 'illegal was committed' and that the US had rebuffed Russian attempts to develop 'common rules acceptable for all, and adhere to them in cyberspace'. Finally, he employed a quintessential whataboutism:

> [W]hen [the Americans] claim that some Russians interfered in the US elections, we tell them … : 'But you are constantly interfering in our political life.' Would you believe it, they are not even denying it. … They said, 'Yes, we do interfere, but we are entitled to do so, because we are spreading democracy, and you are not, and so you cannot do it.' Do you think this is a civilised and modern approach to international affairs?[36]

At least one other State expressed its opinion on this specific case from a legal perspective: Ecuador. This is not surprising, as WikiLeaks' Julian Assange was holed up in its London embassy during the election campaign.[37] On 18 October 2016, Ecuador temporarily restricted Assange's internet access as he was accused of impacting the US election through doxing. An official communiqué elaborated that Ecuador respects the principle of non-intervention in the internal affairs of other states and does not interfere in external electoral processes, nor does it favour any particular candidate.[38]

Several other States have taken a more general position on the application of international law to State cyber-conduct in the context of democratic elections. For example, Australia opined that 'the use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election … would constitute a violation of the principle of non-intervention'.[39] It thereby explicitly (and almost verbatim) endorsed the position of the United Kingdom.[40] Before that, the United States had similarly held that '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

---

[35] Russia, President of Russia, 'Interview to American TV Channel NBC' (10 March 2018) <http://en.kremlin.ru/events/president/news/57027>. See also: *USA v Internet Research Agency LLC et al* (n 16).

[36] Russia (n 35). See also: Russia, Ministry of Foreign Affairs, 'Foreign Minister Sergey Lavrov's Remarks and Answers to Media Questions at a Joint News Conference Following Talks with member of the State Council and Foreign Minister of China Wang Yi' (11 September 2020) <https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4335760> ('absolutely unfounded accusations').

[37] Assange spent seven years in the embassy, but is now jailed in the UK for skipping bail. An extradition hearing pertaining to US charges that he leaked government secrets (unrelated to the 2016 Presidential Election) is ongoing at the time of writing. See: 'Julian Assange Appears in Doc as Extradition Hearing Resumes' *BBC* (7 September 2020) <https://www.bbc.com/news/uk-54060427>.

[38] Ecuador, Ministry of Foreign Affairs and Human Mobility, 'Official Communique' (18 October 2016) <https://www.cancilleria.gob.ec/2016/10/18/comunicado-oficial-sobre-el-caso-julian-assange-2/>.

[39] Australia, Department of Foreign Affairs and Trade, '2019 International Law Supplement – Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace' (2019) <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html>. See also: Australia, Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy' (October 2017) 46 ('The 2016 Presidential Election in the United States focused the world's attention on the potential for cyber-enabled information operations to interfere with processes underpinning democracy. … This behaviour is unacceptable.') and 65 ('Cyber-enabled influence operations during elections can undermine democratic processes. This has the potential to fundamentally distort political debate and democratic outcomes.')

[40] United Kingdom, Attorney General's Office, 'Cyber and International Law in the 21st Century' (23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

violation of the rule of non-intervention'.[41] Most recently, Finland also opined that only some methods of electoral interference display the element of coercion, including vote count manipulation and voter database hacking.[42] New Zealand added cyberoperations that deprive 'a significant part of the electorate of the ability to vote' to that list.[43]

Iran partly agreed with that understanding, yet also seemed to go beyond it:

> Measures like cyber manipulation of elections or engineering the public opinions on the eve of the elections may be constituted of the examples of gross intervention. … Cyber activities paralyzing websites in a state to provoke internal tensions and conflicts or sending mass messages in a widespread manner to the voters to affect the result of the elections in other states is also considered as the forbidden intervention.[44]

Unlike the other States cited above, Iran appears to view widespread measures aimed at 'engineering' public opinion ahead of (or, at least, on the eve of) an election as a prohibited intervention. A little over a month before the Iranian statement was released, the Netherlands also noted that the 'development of advanced digital technologies has given states more opportunities to exert influence outside their own borders and to interfere in the affairs of other states', specifically referring to attempts at influencing election outcomes via social media. However, while the Dutch held that the non-intervention principle indeed 'sets boundaries on this kind of activity', they immediately (and cautiously) noted that the element of coercion at the principle's core has 'not yet fully crystallised in international law'[45] – leaving open the question whether VIOPS would breach it.

On a global level, the United Nations General Assembly (UNGA) adopted a resolution (without vote) on 18 December 2019, wherein it '*[s]trongly condemn[ed]* any manipulation of election processes, coercion and tampering with vote counts, particularly when done by States'.[46] Earlier UNGA resolutions, adopted in the late 1980s and throughout the 1990s, declared that 'activities that attempt, directly or indirectly, to interfere in the free development of national electoral processes … or that intend to sway the results of such processes, violate the spirit and letter of the principles

---

[41] United States, Department of State, 'Remarks on International Law and Stability in Cyberspace' (10 November 2016) <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm>. Israel explicitly concurred with that view, see: R Schondorf, 'Israel's Perspective on Key Legal and Practical Issues concerning the Application of International Law to Cyberspace' (*EJIL:Talk!*, 9 December 2020) <https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/>.

[42] Finland, Ministry of Foreign Affairs, 'Finland Published Its Positions on Public International Law in Cyberspace (15 October 2020) <https://um.fi/current-affairs/-/asset_publisher/qc654PySnjTX/content/suomi-julkisti-n-c3-a4kemyksens-c3-a4-kansainv-c3-a4lisest-c3-a4-oikeudesta-kyberymp-c3-a4rist-c3-b6ss-c3-a4> 3.

[43] New Zealand, Ministry of Foreign Affairs & Trade, 'The Application of International Law to State Activity in Cyberspace' (1 December 2020) <https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf>.

[44] 'General Staff of Iranian Armed Forces Warn of Tough Reaction to Any Cyber Threat' *Nournews* (18 August 2020) <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat> (sic). Iran, like other States, tackles election interference under the heading 'intervention'.

[45] The Netherlands, Ministry of Foreign Affairs, 'Appendix: International Law in Cyberspace' (5 July 2019) <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> 3.

[46] Strengthening the Role of the United Nations in Enhancing Periodic and Genuine Elections and the Promotion of Democratization, UNGA Res 74/158 (18 December 2019) UN Doc A/RES/74/158. Previous, overlapping resolutions were adopted by large majority. See, for example, UNGA Res 72/164 (19 December 2017) UN Doc A/RES/72/164 that was adopted by by 175 votes to none, with 13 abstentions (the latter including China and Russia).

established in the [UN Charter and Friendly Relations Declaration]'.[47] However, unlike the one adopted in 2019, these resolutions with a clearly broader scope encountered significant opposition.

As for the European Union (EU), its position on the legality of (cyber-)VIOPS is somewhat obfuscated. In June 2017, the Council of the EU cautiously expressed the view that 'malicious cyber activities might constitute wrongful acts under international law'.[48] In May 2019, it adopted a framework for restrictive measures (or sanctions) – which the EU considers 'do not rise to the level of internationally wrongful acts but are … unfriendly acts'[49] – to be activated in response to (attempted) 'cyber-attacks with a significant effect', setting a high threshold.[50] Such attacks must be external (e.g., originate from outside the EU) and involve access to or interference with information systems, or constitute data interference or interception.[51] Moreover, they must constitute a 'threat' to Member States, meaning that the attack needs to affect an information system relating to, i.a., critical State functions, 'in particular in the [area] of … governance and the functioning of institutions, including for public elections or the voting process'.[52] In other words, in the context of elections, sanctions can only be imposed if (1) the cyber-attack originates from outside the EU, (2) is of significant scope, and (3) affects the functioning of critical government institutions during an election process. Further watering down its position on VIOPS vis-à-vis international law, the European Commission appeared to suggest that disinformation, including as a threat to democratic processes, is generally 'legal under Union or national law'.[53] The European Parliament, however, adopted a no-holds-barred approach in October 2019 by broadly defining foreign interference in elections as 'including disinformation campaigns on social media to shape public opinion, cyber-attacks targeting critical infrastructure related to elections, and direct and indirect financial support of political actors' and bluntly arguing that such interference 'undermines the right of people to have their say in the

---

[47] UNGA Res 44/147 (15 December 1989) UN Doc A/RES/44/147, para 3. See similar paragraphs in: UNGA Res 45/151 (18 December 1990) UN Doc A/RES/45/151; UNGA Res 46/130 (17 December 1991) UN Doc A/RES/46/130; UNGA Res 47/130 (18 December 1992) UN Doc A/RES/47/130; UNGA Res 48/124 (20 December 1993) UN Doc A/RES/48/124; UNGA Res 49/180 (23 December 1994) UN Doc A/RES/49/180; UNGA Res 50/172 (22 December 1995) UN Doc A/RES/50/172; UNGA Res 52/119 (12 December 1997) UN Doc A/RES/52/119; UNGA Res 54/168 (17 December 1999) UN Doc A/RES/54/168. Moreover, later iterations of the resolution reformulated that paragraph, which then (merely) emphasized the 'free development of the national electoral process in each state': UNGA Res 56/154 (19 December 2001) UN Doc A/RES/56/154, para 4. See similar paragraphs in: UNGA Res 58/189 (22 December 2003) UN Doc A/RES/58/189; UNGA Res 60/164 (16 December 2005) UN Doc A/RES/60/164. For a good overview, see: M Melandri, *Self-Determination, International Law and Post-Conflict Reconstruction* (Routledge 2019) Table A.1.

[48] Council of the EU, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")' (7 June 2017) <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf>.

[49] Council of the EU, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities' (9 October 2017) <https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf> 5.

[50] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States [2019] OJ L 129 I/13. See also: Council Regulation (EU) 2019/796 of 17 May 2019 concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States [2019] OJ L 129 I/1.

[51] Council Decision (CFSP) 2019/797 (n 50) art 1(2) and (3). For the factors determining 'significant effect', see ibid art 3.

[52] ibid art 1(4)(c). It has since imposed sanctions for cyber-attacks against the Organisation for the Prohibition of Chemical Weapons and those known as 'WannaCry', 'NotPetya' and 'Operation Cloud Hopper', see: Council of the EU, 'EU Imposes the First Ever Sanctions against Cyber-Attacks' (30 July 2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/>.

[53] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, 'Action Plan against Disinformation' (5 December 2018) <https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf> 1. The distinction was made with 'illegal content on-line', including 'information relating to terrorism, child sexual abuse, illegal hate speech or infringements of consumer protection laws', see: 'Commission Recommendation of 1.3.2018 on Measures to Effectively Tackle Illegal Content Online' (1 March 2018) <https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online>.

governance of their country, directly or through freely chosen representatives, as enshrined in the Universal Declaration of Human Rights' and 'constitutes a violation of international law, *even when there is no use of military force, threat to territorial integrity or threat to political independence*'.[54]

In 2018, the influential Group of Seven (G7) also labelled '[f]oreign actors seeking to undermine democratic institutions and processes through coercive, corrupt, covert or malicious means' as a 'strategic threat', while providing examples similar to the facts of the case study under review.[55] This position was, at least in part, adopted in response to heightened concerns over 'a pattern of earlier irresponsible and destabilizing Russian behaviour, including interference in countries' democratic systems'.[56] It was moreover reiterated in 2019, by emphasizing a determination to 'work collaboratively to reinforce our democracies against illicit and malign behavior and foreign hostile interference by state and non-state actors'.[57] On 12 December 2018, one of the G7 States, France, also launched the Paris Call for Trust and Security in Cyberspace, aimed at attracting support from both State and private entities. Notably, the signatories affirmed a willingness to strengthen their 'capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities'.[58]

Two important elements pertaining to States' *opinio juris* on VIOPS stand out from this overview: First, States and international organizations are increasingly concerned about the rise of voter influence operations,[59] fuelled by the widespread availability of low-cost but high-impact cybercapabilities. Second, while select examples of State action targeting democratic elections abroad are generally labelled as unlawful under the principle of non-intervention (i.e., coercing individual voters, altering election results or interfering with critical State functions), others are more commonly described as illicit or malicious(/malign) and trample on entrenched but voluntary (or non-legally binding)

---

[54] European Parliament, Resolution on 'Foreign Electoral Interference and Disinformation in National and European Democratic Processes' (10 October 2019) 2019/2810(RSP) <https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_EN.pdf> paras B and 3 (emphasis added).

[55] G7, 2018 Summit Canada Presidency, Joint Statement of Foreign and Security Ministers, 'Defending Democracy – Addressing Foreign Threats' (23 April 2018) <http://www.g7.utoronto.ca/foreign/180423-democracy.html>. The G7 is an informal grouping of seven of the world's most advanced economies, consisting of: Canada, France, the United States, the United Kingdom, Germany, Japan and Italy. The European Union is a non-enumerated member.

[56] Canada, Global Affairs Canada, 'G7 Foreign Ministers' Statement' (16 April 2018) <https://www.canada.ca/en/global-affairs/news/2018/04/g7-foreign-ministers-statement.html>.

[57] G7, 2019 Biarritz Summit, 'Biarritz Strategy for an Open, Free and Secure Digital Transformation' (26 August 2019) <https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf> para 4.

[58] The call has been backed by 1104 entities, including 78 States: France, Diplomatie, 'Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace' <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in>. See also: APB Laudrain, 'Avoiding a World War Web: The Paris Call for Trust and Security in Cyberspace' (*Lawfare*, 4 December 2018) <https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace>.

[59] See, for example: Levin (n 3 and 5); United States, Senate Committee on Foreign Relations, 'Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security' (10 January 2018) <https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf>; S Davis, NATO, 'L'ingérence de la Russie dans les élections et les référendums des pays de l'alliance' (18 November 2018) 181 STC 18 F fin; F Hanson et al, Australian Strategic Policy Institute 'Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections' (15 May 2019) <https://www.aspi.org.au/report/hacking-democracies>; European Commission, High Representative of the Union for Foreign Affairs and Security Policy, 'Report on the Implementation of the Action Plan against Disinformation' (14 June 2019) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN>. For a more general overview, see: Levin (n 5); D Shimer, *Rigged: America, Russia, and One Hundred Years of Covert Electoral Interference* (Alfred A. Knopf 2020).

norms of behaviour. Admittedly, the reactions by Ecuador, Iran and the European Parliament (but *not* that of the EU's executive branch) do not fit neatly in this summary.

2.3 Voter influence operations and the 2020 US Presidential Election

But before moving to the international legal framework as it applies to VIOPS, a brief overview of the state-of-affairs regarding foreign meddling in the 2020 US President Election campaign is in order. On 24 July 2020, the Director of the US National Counterintelligence and Security Center (NCSC) confirmed that the same tactics were deployed in this election cycle as the ones under review.[60] Indeed, in a second statement he warned that foreign States may seek to 'continue to compromise our election infrastructure for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results'.[61] More specifically, he acknowledged that China appears to prefer an 'unpredictable' President Trump *not* to win re-election and that Iran was also working to undermine the President. Conversely, Russian measures were designed to defame the Democratic standard-bearer, former Vice-President Joe Biden. A little over a month later, the Director of the Federal Bureau of Investigation (FBI) confirmed that his task force was confronting global adversaries. He agreed that Russia was working to denigrate Biden, but noted that the measures were limited to misinformation campaigns – unlike in 2016, when 'the most serious interference efforts involved hacking Democrats' emails and state election systems'.[62]

Then, on 21 October 2020, the US Director of National Intelligence shared the discovery of specific foreign activity designed to influence public opinion. For example, Iran was thought to be the author of 'spoofed' emails aimed at intimidating voters, inciting social unrest and damaging President Trump. Allegedly, it also released a video suggesting that voters could cast fraudulent ballots even from overseas. And while Russia was not accused of any specific shenanigans, an unsubstantiated news article suggesting that Joe Biden as Vice-President had shaped foreign policy in Ukraine to benefit his son, who sat on the board of a Ukrainian energy company, had Russian fingerprints all over it. Be that as it may, the US National Security adviser also announced that his Russian counterpart had 'committed' to refrain from interfering with the US Election Day.[63]

---

[60] United States, Director of National Intelligence, 'Statement by NCSC Director William Evanina: 100 Days until Election 2020' (24 July 2020) <https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020>. See also: Section 2.1.

[61] United States, Director of National Intelligence, 'Statement by NCSC Director William Evanina: Election Threat Update for the American Public (7 August 2020) <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>.

[62] D Barrett, 'FBI Director Affirms Russia's Aim to "Denigrate" Biden ahead of Election' *The Washington Post* (18 September 2020) <https://www.washingtonpost.com/national-security/wray-fbi-election-security-threats-hearing/2020/09/16/4461526e-f869-11ea-a275-1a2c2d36e1f1_story.html>. But see: United States, Department of Homeland Security, 'Homeland Threat Assessment' (October 2020) <https://assets.documentcloud.org/documents/7223004/DHS-Homeland-Threat-Assessment-Oct-2020.pdf> 9.

[63] United States, Director of National Intelligence, 'DNI John Ratcliffe's Remarks at Press Conference on Election Security' (21 October 2020) <https://www.dni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security>; N Bertrand, 'Hunter Biden Story Is Russia Disinfo, Dozens of Former Intel Officials Say' *Politico* (19 October 2020) <https://www.politico.com/news/2020/10/19/hunter-biden-story-russian-disinfo-430276>; D Sanger, 'Russians "Have Committed" to Not

3 Questions of legality in 'meat'- and cyberspace

3.1 The principle of sovereign equality

The United Nations is based on the principle of sovereign equality of all its Members. That principle entails that each State enjoys the rights inherent in full sovereignty, including the inviolability of its territorial integrity and political independence.[64] Max Huber, the sole arbitrator in the *Island of Palmas* case, famously held that sovereignty signifies independence, or the right to exercise the functions of a State within a territory 'to the exclusion of any other State'.[65] In the seminal *Lotus* case, the Permanent Court of International Justice (PCIJ) confirmed that no State may exercise its power in any form in the territory of another State 'failing the existence of a permissive rule to the contrary'.[66] Its successor, the International Court of Justice (ICJ), determined that 'respect for territorial sovereignty is an essential foundation of international relations' and 'international law requires political integrity to also be respected'.[67] Finally, the UN Group of Governmental Experts (UN GGE) agreed that State sovereignty also applies to 'the *conduct* by States of ICT-related activities and to their *jurisdiction* over ICT infrastructure within their territory'.[68]

Drilling down to the substance of the principle, Akehurst commented that an act performed by one State in the territory of another without consent only violates international law if it 'represents a usurpation of the [latter's] sovereign powers'. Usurpation can be determined by the *nature* of the act (i.e., acts only State officials are entitled to perform, such as collecting taxes) or its *purpose* (e.g., seeking information in the territory of another State to enforce tax laws). Moreover, covertly sending State officials across borders equally violates territorial sovereignty as it contravenes immigration policy.[69] Similarly, Jennings and Watts distinguish between two aspects of sovereignty (in addition to independence): territorial(*/ dominium*) and personal(*/ imperium*) authority. The former comprises the power of a State to 'exercise supreme authority over all persons and things within its territory', whereas the latter denotes a similar competence over citizens at home and abroad.[70] State sovereignty is violated when acts involve the exercise of 'sovereign authority or derogate from the sovereign authority of the territorial state'. Examples are

---

Interfering in Elections, Trump Aide Insists' *The New York Times* (4 October 2020) <https://www.nytimes.com/2020/10/04/us/politics/russia-election-interference.html>.

[64] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 2(1); Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, UNGA Res 2625 (XXV) (24 October 1970) UN Doc A/RES/2625(XXV) 124.

[65] *Island of Palmas case (Netherlands, United States of America)* (1928) II RIAA 829, 838.

[66] *The Case of the S.S. "Lotus" (France v Turkey)* (Merits) [1927] PCIJ Rep Series A No 10, 18.

[67] *The Corfu Channel Case (United Kingdom v Albania)* (Merits) [1949] ICJ Rep 4, 35; *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 202.

[68] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174, para 27 (emphasis added); UNGA Res 70/237 (23 December 2015) UN Doc A/RES/70/237. ICT stands for Information and Communications Technologies, i.e., cyber.

[69] M Akehurst, 'Jurisdiction in International Law' (1972-3) 46 BYIL 145, 146-50.

[70] R Jennings and A Watts, *Oppenheim's International Law*, vol 1 (9th edn, OUP 2008) para 117, 382. See also: K Bannelier, '"Rien que le *lex lata*?" Étude critique du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations' (2017) Annuaire français de droit international 121, 138 (note 101).

sending agents into foreign territory to conduct clandestine operations (*dominium*) or preventing alien residents from fulfilling military service in their home State (*imperium*).[71]

But how, then, to apply that principle in cyberspace? According to the authors of the *Tallinn Manual 2.0*, an insightful document prepared by an international group of experts with the input of States,[72] two criteria need to be taken into account when assessing whether *remote* cyber operations that manifest on a State's territory violate its sovereignty: (1) the degree of infringement upon the target State's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions. Fully in line with the abovementioned case law and doctrine, the first criterion is based on the premise that a State controls access to its sovereign territory, while the second relies on the sovereign right to exercise State functions therein to the exclusion of any other.[73]

On the one hand, a State's territorial integrity is infringed if the cyber operation results in physical damage or injury, or the loss of infrastructure functionality necessitating repair. The experts could not agree on the (il)legality of operations below that threshold, e.g., causing cyber infrastructure or programs to operate differently, altering or deleting data, emplacing malware into a system, and causing a temporary but significant loss of functionality. Inherently governmental functions, on the other hand, are those that are exclusively reserved to the territorial State and cannot be performed by non-governmental entities. One (relevant) example would be the *conduct* of elections so that interfering with that function (e.g., by disrupting election hardware) constitutes a sovereignty violation. The same would not hold for, say, transmitting propaganda.[74]

But a broader debate emerged afterwards on the existence of sovereignty as a primary *rule*, rather than a *principle*, in cyberspace. Sovereignty-as-a-principle was defended by Corn and Taylor, who stated that '[t]he principle of sovereignty is universal, but its application to the unique particularities of the cyberspace domain remains for states to determine through state practice and/or the development of treaty rules'.[75] That view was explicitly endorsed by the UK Attorney-General, who argued that his Government's position was 'therefore that there is no such rule as a matter of current international law'.[76] After reviewing 11 case studies involving cyber operations since 2013, Efrony and Shany did not disprove that position (but without endorsing it either).[77] Other scholars did support sovereignty-

[71] ibid 385-90, para 119. They provide plenty of other practical examples.
[72] M Schmitt and L Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017). The manual arguably qualifies as *subsidiary* means for the determination of international law under art 38(1)(d) of the ICJ Statute. But for a critical review, including on the expert body's composition and methodology, see: Bannelier (n 70).
[73] ibid 20 (para 10).
[74] ibid 20-4 (paras 10-22) and 26 (para 29). Agreeing with the idea that it required a certain level of damage (higher than that for a violation of the due diligence principle) is: M Forteau, 'Les seuils de gravité d'une cyberattaque' in M Grange and A Norodom, *Cyberattaques et droit international: Problèmes choisis* (Pedone 2018) 33.
[75] G Corn and R Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207, 210. See also: S Watts and T Richard, 'Baseline Territorial Sovereignty and Cyberspace' (2018) 22 Lewis & Clark Law Review 771, 827ff.
[76] United Kingdom (n 40).
[77] Efrony and Shany (n 8) 640-1.

as-a-rule, relying on State practice, *opinio juris*, international case law, and its understanding in international fora.[78] However, the debate does not appear conclusively settled at the time of writing.[79]

Another difficult question which flows from that conundrum is one that also frustrated the *Tallinn Manual 2.0*'s authors: What are the specific edicts that flow from sovereignty as either a principle or a rule? Or, specified further for our purposes: Do remote cyberoperations that lack territorial impact but intrude on cyberinfrastructure constitute a violation of the principle of sovereign equality?

Three distinct approaches seem to have formed in response to that question.[80] The first, *denialist* approach is propagated by the United Kingdom, arguing that while sovereignty is 'fundamental to the international rules-based system', it cannot 'currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention'. Put bluntly, the UK does not believe in a 'cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent'.[81]

The second, *conservative* approach derives from States' scattered and ambiguous practice as well as their wait-and-see attitude. Efrony and Shany helpfully explain:

> Given the doubts that many state officials seem to have as to the contents of regulation … in cyberoperations, the uneven capacities of states in this field, and the lack of effective international institutions for attributing responsibility and applying international law norms, it is not surprising that efforts to regulate cyberspace … meet some skepticism and resistance, and shape only to a limited degree state practice.[82]

The idiosyncrasies of cyberspace, and States' ongoing debate in this context,[83] result in an area of newly emerging international law regulation with many grey areas in need of consolidation before operating as positive international law. Its architects are still in the process of construing 'a concrete cyber legal order' out of what currently amounts

---

[78] M Schmitt and L Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 TexLRev 1639, 1649-68; Watts and Richard (n 75). See also: R Buchan, *Cyber Espionage and International Law* (Hart 2019) 49ff.

[79] For an overview of diverging national positions, see: Organization of American States, Report by Duncan Hollis, 'Improving Transparency: International Law and Cyber Operations – Fifth Report' (7 August 2020) CJI/doc.615/20 rev. 1, 29-45 and P Roguski, The Hague Program for Cyber Norms, 'Application of International Law to Cyber Operations: A Comparative Analysis of States's Views' (March 2020) <https://www.thehaquecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views> 4-7.

[80] However, not all States have taken a clear position on this issue. See, for example: Australia (n 39); Germany, Federal Foreign Office, 'Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy' (18 May 2015) <https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832>; Estonia, President, 'President of the Republic at the Opening of CyCon 2019' (29 May 2019) <https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html>.

[81] United Kingdom (n 40).

[82] Efrony and Shany (n 8) 653.

[83] For an overview of UN efforts, see: <https://dig.watch/processes/un-gge#view-7541-3>.

to a mere blueprint.[84] Consequently, the Netherlands cautiously adopted a *de minimis* approach, very much in line with that suggested by the Tallinn Manual authors:

> States have an obligation to respect the sovereignty of other states and to refrain from activities that constitute a violation of other countries' sovereignty. … [T]he precise boundaries of what is and is not permissible have yet to fully crystallise. This is due to the firmly territorial and physical connotations of the traditional concept of sovereignty. … In general … a violation of sovereignty is deemed to occur if there is 1) infringement upon the target State's territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another state. The precise interpretation of these factors is a matter of debate.[85]

This is supported by other States, including, *a contrario*, by the United States even if its attitude remains somewhat equivocal.[86] For example, in 2016, the US Department of State Legal Adviser noted that

> remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law. … This is perhaps most clear where such activities in another State's territory have no effects or *de minimis* effects. … Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study … .[87]

Four years later, the US Department of Defense (DOD) General Counsel echoed this understanding:

> [T]here is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law *generally* prohibits such non-consensual cyber operations in another State's territory. … [I]t does not appear that there exists a rule that *all* infringements on sovereignty in cyberspace *necessarily* involve violations of international law.[88]

Despite all the 'hedging, fence-sitting language',[89] the US position thus seems to fit better with this second approach, admitting that cyberoperations which have territorial consequences of a certain magnitude may well violate the principle of sovereign equality.

Finally, a third, *speculative* approach – also known as the penetration-based one – relies on the exclusive jurisdiction by the territorial State over ICT-infrastructure within its territory and the data it contains (as confirmed by the UN GGE[90]) implying that its digital penetration by other States is unlawful.[91] Consequently, non-consensual intrusions in

---

[84] N Tsagourias, 'The Slow Process of Normativizing Cyberspace' (2019) 113 AJIL Unbound 71, 71-2.
[85] The Netherlands (n 45) 2-3, explicitly endorsing the Tallinn Manual (n 72-74). The term is coined by Roguski ((n 79) 4).
[86] See also: Czech Republic, Cybersecurity Department, 'Statement by Special Envoy for Cyber Space' (11 February 2020) <https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf>; Guyana (Hollis report (n 79) para 41); Finland (n 42) and New Zealand (n 43).
[87] United States (n 41).
[88] United States, Department of Defense, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference' (2 March 2020) <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/> (emphasis added).
[89] Milanovic and Schmitt (n 8) 5.
[90] 2015 UN GGE Report (n 68) paras 27-8.
[91] The term is coined by Roguski ((n 79) 4). The view is eloquently set out by Buchan ((n 78) 51-5).

both 'meat'- and cyberspace constitute a violation of sovereignty-as-a-rule. This cutting-edge approach is promoted by France:

> Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.[92]

On balance, however, the speculative approach is unconvincing for three reasons: First, UN efforts to specify international norms applicable in cyberspace originated from the understanding that 'we have only begun to develop the norms, laws and modes of cooperation needed for this new information environment'.[93] The 2013 UN GGE report labels that exercise as essential, but admits that '[c]ommon understandings on how such norms shall apply to State behaviour … requires further study'.[94] And while 'slow yet meaningful progress' was made, that progress came to a grinding halt in 2017.[95] In other words, this is very much still a work in progress.

Second, and in addition to the absence of widely available and explicitly supportive *opinio juris*, the American, British and Russian reactions appear to forcefully undermine at least the most progressive interpretation.[96] In a speech celebrating the *Tallinn Manual*'s first 'anniversary' the Dutch Foreign Affairs Minister astutely noted:

> Of course, the Tallinn Manual doesn't provide all the answers. It's not an official document, and the Netherlands doesn't necessarily agree with everything in it. … Nor is it simple. Issues like state responsibility are complicated enough in the 'real' world, let alone the 'virtual' world. *In no small part, because there they represent uncharted legal territory.*[97]

Third, even proponents of the speculative approach admit that its status as *lex lata* is unclear. After an extensive review of State practice, *opinio juris* and doctrine, Navarrete and Buchan only coded 'remote access cyber espionage'

---

[92] France, Ministry of Armed Forces, 'International Law Applied to Operations in Cyberspace' (4 October 2019) <https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international>. Moreover, the French define a cyberattack as a 'deliberate offensive or malicious action carried out via cyberspace and *intended to cause damage (in terms of availability, integrity or confidentiality) to data* or the systems that treat them' (ibid, 18 (emphasis added)). The French position appears inspired by a study carried out by Delerue, see: 'Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations' (November 2017) <http://francoisdelerue.eu/wp-content/uploads/2020/01/20171129_NP_F-Delerue_Analyse-Manuel-Tallinn-2-0.pdf>. The Iranian position (n 44) also seems to follow this approach, as does that of Guatemala (Hollis report (n 79) para 41). Moreover, in 2013, MERCOSUR strongly rejected 'the interception of telecommunications and the acts of espionage carried out in our countries', which was considered to 'violate[its] sovereignty', see: Annex to the Note Verbale Dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations Addressed to the Secretary-General (29 July 2013) UN Doc A/67/946, 2. This was endorsed by Cuba later that year, speaking on behalf of all CELAC members: Statement by Cuba, UNGA General Debate, 68th Session (26 September 2013) <https://gadebate.un.org/en/68/cuba>. But: compare with contradictory positions seemingly taken by some of these same States in the Hollis report (n 79).

[93] UN GGE Report (30 July 2010) UN Doc A/65/201, 4 (foreword by UN Secretary-General, at the time, Ban Ki-moon).

[94] UN GGE Report (24 June 2013) UN Doc A/68/98, para 16.

[95] M Schmitt and L Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (*Just Security*, 30 June 2017) <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>. But see the UN efforts in this respect (n 83). See also: 2015 UN GGE Report (n 68) and (n 80).

[96] United Kingdom (n 40); Watts and Richard (n 75); Russia (n 35).

[97] 'Keynote by HE Mr. Stef Blok MA, Minister of Foreign Affairs' (2018) 111 Militair Rechtelijk Tijdschrift <https://puc.overheid.nl/mrt/doc/PUC_248137_11/1/> (emphasis added).

as '*possibly* in breach of the principle of territorial integrity'.[98] Similarly, there was an insurmountable disagreement among the *Tallinn* experts on whether a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty.[99] One of these experts separately noted that momentum was building behind the view that 'mere compromises or thefts of data are not violations of sovereignty, but rather routine facets of espionage and competition among States'.[100] Another acknowledged that it was 'impossible to draw definitive red lines regarding cyber election meddling in the context of the territorial aspect of sovereignty, except with respect to situations causing physical damage or at least a significant impact on functionality'.[101]

In the end, it is thus fair to say that this understanding argues against the most expansive interpretation of sovereignty in cyberspace. While State sovereignty certainly prohibits *territorial (physical)* non-consensual intrusions by foreign State agents, the same does not necessarily apply to *remote* cyberactivities. However, a sovereignty violation arguably does occur if the *remote* State cyberaction has direct *territorial* effects (damage or injury, or the serious loss of infrastructure functionality) or interferes with an inherently governmental function.[102] After all, a cardinal international legal rule outlawing certain consequences can be thought to apply irrespective of the means employed – thereby knocking out the *denialist* approach also.[103] It makes little sense to argue that the prohibition on territorial infringement and interference with governmental functions only applies in 'meat'- but not in cyberspace.

Admittedly, this is a rather restrictive reading of international law and one that is subject to erosion.[104] But it is submitted that sovereignty has, at least for not the moment, not been extended by States to include banning remote, non-consensual intrusions lacking territorial impact. Where does this leave us with regard to the legality of the three specific actions of the case study? The overview of publicly known facts in Section 2.1 clarifies that nearly all acts involved remote ICT-activities without physical intrusion on United States territory – meaning they cannot qualify as sovereignty violations. That applies most clearly to the spread of propaganda and disinformation through social media, the release of private documents, and the reconnaissance hacking of election-related infrastructure with no indication of system-manipulation or data-altering. Even malware was installed by the unwitting victims themselves, similar to how American voters were nudged into organizing political rallies. Moreover, no remote cyberoperations took place that interfered with the conduct of elections *sensu stricto*, i.e., the ability of the American government to

---

[98] I Navarrete and R Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51 CornellIntLJ 897, 953 (emphasis added). See also ibid

[99] *Tallinn Manual 2.0* (n 72) 21 (para 14).

[100] Watts (n 8).

[101] Schmitt (n 8) 45.

[102] C Marxsen, 'Territorial Integrity in International Law: Its Concept and Implications for Crimea' (2015) 75 ZaöRV 7, 12.

[103] See (n 64-74). Compare with the effects-based approach used to qualify a cyber operation as a prohibited use of force: *Tallinn Manual 2.0* (n 72) 330-7; International Law Association, 'Final Report on Aggression and the Use of Force' (2018) <http://www.ila-hq.org/images/ILA/DraftReports/DraftReport_UseOfForce.pdf> 25; The Netherlands, AIV and CAVV, 'Cyber Warfare' (December 2011) <https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare> 21; Australia (n 39); United Kingdom (n 40). For a more expansive view, see: M Schack, 'Did the US Stay "Well Below the Threshold of War" with Its June Cyberattack on Iran?' (*EJIL:Talk!*, 2 September 2019) <https://www.ejiltalk.org/did-the-us-stay-well-below-the-threshold-of-war-with-its-june-cyberattack-on-iran/>.

[104] See, specifically (n 92).

successfully organize the election.[105] Finally, those tactics do not seem to have changed dramatically in the 2020 election cycle – if at all.[106]

On the other hand, the covert IRA intelligence-gathering mission on US soil whereby two employees obtained immigrant visa under false pretences would seem to qualify as a(n almost literal) violation of territorial sovereignty.[107] A related query is then whether transgressing against other relevant US legislation, such as that related to wire and bank fraud or the Foreign Agents Registration Act (FARA), would similarly qualify as sovereignty violations. That does not seem to be the case. In these latter cases, Russia is not carrying out acts that *usurp* or *derogate from* the exercise of sovereign powers of the United States – either by performing functions that only US officials are entitled to perform or by enforcing Russian legislation abroad.[108] The opposite interpretation is much less cogent, as any breach of domestic legislation by a foreign State agent would then contravene sovereignty even if it pertained to something as minimal as a traffic violation. Indeed, according to the US DOD General Counsel:

> Many of the techniques and even the objectives of intelligence and counterintelligence operations are similar to those used in cyber operations. Of course, most countries, including the United States, have *domestic* laws against espionage, but international law, in our view, does not prohibit espionage *per se even when it involves some degree of physical or virtual intrusion into foreign territory.*[109]

The better view is thus focused on the distinction comparable to that between wilful disobedience of national legislation by a third State (domestic law violation) and the appropriation of power (international law violation).

Of those academic commentators looking at the principle of sovereign equality, only a few assessed that it was likely violated by the Russian actions under review. Most explicitly, Schmitt noted that the social media campaign manipulated voters' ability to 'assess the messages in coming to their own decision' by 'feigning the source thereof'. Supposedly, it was this manipulation that 'tipped the scales' and, therefore, 'constituted unlawful interference'. Moreover, because the GRU not only *exfiltrated* private information from Democratic party officials, but later *weaponized* it by releasing it at 'critical points in the election', he considered the qualification as interference 'at least somewhat supportable'. He concluded that, taken together, 'the most legally sustainable and persuasive position is that [those] aspects of the Russian influence campaign violated U.S. sovereignty'. However, even Schmitt admitted that his conclusion – which, in any case, has a *lex ferenda* nature – was 'far from unassailable'.[110] Similarly, Moynihan argued that 'the highly intrusive nature of the Russian operation, and its extensive reach in terms of numbers of the population, suggests that it could constitute a violation of sovereignty' but immediately added that 'the lack of

---

[105] An example would be the 'temporary distributed denial of service attack against election machinery that rendered it impossible for voters in a particular district to cast their votes', see Schmitt (n 8) 46.
[106] See text accompanying (n 62).
[107] *USA v Internet Research Agency LLC et al* (n 16) paras 27 and 30; see also text accompanying (n 69 and 71).
[108] See text accompanying (n 64-71).
[109] See US DOD (n 88) (emphasis added).
[110] Schmitt (n 8) 47.

agreement of criteria for violation of sovereignty, including what, if any, effects should be taken into account, makes the assessment difficult'.[111]

Conversely, the editors of the Interactive Cyber Toolkit assessed that only the hack-and-leak of private emails belonging to an election candidate's campaign team may qualify as a sovereignty violation – but only if a State 'obtained them in a cyber operation conducted by its agents present in [the target State's] territory'.[112] That is an altogether different question and, in any event, does not appear to be the case here. Other authors – e.g., Ohlin, Crootof and Sander – did not find a sovereignty violation either,[113] a point of law with which this article agrees, albeit for slightly different reasons as explained above.

3.2 The principle of non-intervention and right to self-determination

Even more than sovereignty, almost all authors commenting on this case study discussed the legality of its underlying actions in relation to the principle of non-intervention. This principle prohibits States from intervening 'directly or indirectly, for any reason whatever, in the internal or external affairs of any other State'. It moreover proscribes using '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'. The principle was designed to protect each *State's* 'inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State', and it is this inalienable right that is at the core of our legal study.[114]

The same right is moreover found as part of *peoples'* right to self-determination under international law: 'all peoples have the right freely to determine, without external interference, their political status and to pursue their economic, social and cultural development, and every State has the duty to respect this right in accordance with the provisions of the [UN] Charter'.[115] This conceptual link between non-intervention and self-determination is by no means a coincidence, as evidenced from the Friendly Relations Declaration's *travaux préparatoires*.[116] Indeed, from the perspective of the people of an independent State as a whole, the right to self-determination 'takes the well-known form of the rule preventing intervention in the internal affairs of a State'.[117] In sum, and from that point of view

[111] Moynihan (n 8) 43.
[112] Interactive Cyber Toolkit (n 8) Scenario 01: Election interference.
[113] While Ohlin discussed sovereignty primarily in the context of the principle of non-intervention, see Section 3.2 below, Crootof noted that 'the DNC hack alone might not qualify as a violation of U.S. sovereignty, because nothing was damaged' (Crootof (n 8) 629). Moreover, Sander observed that 'States may not wish to advance an expansive notion of sovereignty for fear that doing so would limit their own cross-border covert intelligence operations, whilst also restricting their freedom to take action against hostile cyber operations' (Sander (n 8) 53-4).
[114] Friendly Relations Declaration (n 64) 123. See also *Tallinn Manual 2.0* (n 72) 315 (para 10).
[115] Friendly Relations Declaration (n 64) 123.
[116] (Second) Report of the Special Committee on Principles of International Law concerning Friendly Relations and Co-operation among States, Rapporteur: W. Riphagen (Netherlands) (27 June 1966) UN Doc A/6230, para 480.
[117] J Crawford, *The Creation of States in International Law* (2nd edn, OUP 2007) 126.

specifically, non-intervention and self-determination are two sides of the same coin – and will therefore be discussed in a single section.

Doctrine has long since accepted that the inalienable right to freely choose a political, cultural, economic and social *system* or *status* necessarily includes the right to freely choose a *government*.[118] Building upon that argument, and referring to pertinent UN Security Council resolutions, Dam-de Jong then evidenced that in practice 'elections generally serve as the principal means of ascertaining that a people has been able to freely exercise its right to selfdetermination', even if they are but one way of doing so.[119] Put differently, the people of a State generally exercise their right to self-determination by choosing their political leadership, one way or another.[120]

The exercise of that right, belonging to the State's *domaine réservé*,[121] is then protected from external *coercive* interference by the non-intervention principle. According to the ICJ, it is this element of coercion that 'defines, and indeed forms the very essence of, prohibited intervention'.[122] Unfortunately, the ICJ provides only limited practical examples of coercion: the direct (military action) and indirect (support for subversive or terrorist armed activities) use of force.[123] However, while using force may well be coercive by definition, the concept does not hinge solely on the *specific* measure employed. Indeed, the Friendly Relations Declaration outlaws the use of *any type of* measure if aimed at the subordination of the target State and designed to 'secure from it advantages of any kind'.[124]

Another route offered by (classical) doctrine is that interference is coercive when dictatorial, i.e., it in effect deprives the State 'of control over the matter in question'.[125] This interpretation of coercion as something akin to *force majeure* is echoed by the International Law Commission (ILC) in the context of Article 18 ARSIWA (on 'Coercion of another State').[126] There, the ILC set an exceptionally high threshold, since '[n]othing less than conduct which forces the will of the coerced State will suffice [for the responsibility of the coercing State] … . It is not sufficient that compliance with the obligation is made more difficult or onerous'.[127] However, State practice in this extreme case is uncommonly rare,[128] leading some authors to more mildly claim that acts 'of a certain magnitude' likely qualify as coercive.[129]

---

[118] R Higgins, *Problems and Process: International Law and How We Use It* (OUP 1995) 119-20.
[119] D Dam-de Jong, *International Law and Governance of Natural Resources in Conflict and Post-Conflict Situations* (CUP 2015) 74.
[120] G Fox, 'Democracy, Right to, International Protection' (2008) MPEPIL 773; N Petersen, 'Elections, Right to Participate in, International Protection' (2012) MPEPIL 785.
[121] K Ziegler, 'Domaine Réservé' (2013) MPEPIL 1398; *Nationality Decrees Issued in Tunis and Morocco* (Advisory Opinion) [1923] PCIJ Rep Series B No 4, 23-4; ICJ *Nicaragua* case (n 67) para 205.
[122] ICJ *Nicaragua* case (n 67) para 205.
[123] ibid.
[124] See text accompanying (n 114). See also: Helal (n 8) 5 and 43-4.
[125] Jennings and Watts (n 70) para 129, 432.
[126] ARSIWA (n 9) art 18 jo. 23.
[127] 'Draft Articles on Responsibility of States for Internationally Wrongful Acts: Commentaries' (2001) II(2) YILC 30, 69(2). See also: A Tzanakopoulos, 'The Right to be Free from Economic Coercion' (2015) 4 CJIntl&CompL 616, 622-3.
[128] ARSIWA Commentary (n 127) 70(7); Tzanakopoulos (n 127); J Fry, 'Coercion, Causation, and the Fictional Elements of Indirect State Responsibility' (2007) 40 VandJTransnatlL 611, 621-7.
[129] M Jamnejad and M Wood, 'The Principle of Non-Intervention' (2009) 22 LJIL 345, 348.

Similarly, the *Tallinn Manual 2.0* also claims that coercion refers to 'an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act [or refrain from acting] in an involuntary manner' with respect to areas of exclusive domestic jurisdiction.[130] Interestingly, they then move away from the traditional interpretation in doctrine by accepting the illegality of *attempted* and *threatened* interventions as well. First, the experts correctly opine that 'the fact that a coercive cyber operation fails to produce the desired outcome has no bearing' on its legality.[131] This aligns well with the *texte clair* of the Friendly Relations Declaration and avoids the no-win situation for the target State of either suffering but resisting the (non-forcible, non-dictatorial) pressure (no intervention) or submitting to that pressure and subordinating the exercise of its sovereign powers (intervention).[132] Second, the Tallinn experts considered the *threat* of a coercive cyber operation that intrudes on the target State's *domaine réservé* a prohibited intervention also, regardless of its ultimate success, similar to how the threat to use force is included in Article 2(4) of the UN Charter.[133] On the other hand, they distinguish coercion from 'persuasion, criticism, public diplomacy, propaganda … and the like' since those latter acts 'merely involve … influencing (as distinct from factually compelling) the voluntary actions of the target State'.[134] Not coincidentally, this largely matches with States' *opinio juris* on VIOPS as summarized above: while election *manipulation* (e.g., coercing individual voters, altering election results or tampering with election infrastructure) is labelled unlawful, election *meddling* is rather thought of as malicious or unfriendly State behaviour that does not, necessarily, violate international law.[135]

In sum, a State that forcibly or dictatorially interferes with another State's *domaine réservé* – or threatens or attempts to do just that – violates the principle of non-intervention, which is 'part and parcel of customary international law'.[136] That domain of exclusive domestic jurisdiction indisputably contains the State and its people's right to freely choose their government.[137] The exercise of that right has multiple facets. Generally, it pertains to the choice of political status, form of constitution and government (as well as a corresponding duty for the State to describe the 'constitutional and political processes' that make such a choice possible).[138] But it is also closely related to the right

[130] *Tallinn Manual 2.0* (n 72) 317-18 (paras 18-19). See also ibid 314-17 (paras 7-16) and (n 121).
[131] ibid 322 (para 29).
[132] Friendly Relations Declaration (n 64) 1236: 'Consequently, armed intervention and all other forms of interference or *attempted threats* against the personality of the State or against its political, economic and cultural elements are in violation of international law.' (emphasis added); Helal (n 8) 5-6 and 44-7. See also: A Hofer and L Ferro, 'Sanctioning Qatar: Coercive Interference in the State's Domaine Réservé?' (*EJIL:Talk!*, 30 June 2017) <https://www.ejiltalk.org/sanctioning-qatar-coercive-interference-in-the-states-domaine-reserve/#more-15383>.
[133] *Tallinn Manual 2.0* (n 72) 322-3 (para 30).
[134] ibid 318-19 (para 21). See also text accompanying (n 74). On the regulation of propaganda in international law more generally, see: E De Brabandere, 'Propaganda' (2019) MPEPIL 978; Jennings and Watts (n 70) para 122, 403-6; L Preuss, 'International Responsibility for Hostile Propaganda against Foreign States' (1934) 28 AJIL 649.
[135] See Section 2.2.
[136] ICJ *Nicaragua* case (n 67) para 202.
[137] See text accompanying (n 114-121).
[138] Ziegler (n 121) para 5f; ICJ *Nicaragua* case (n 67) para 263; UN Human Rights Committee, 'The Right to Self-Determination of Peoples (General Comment 12)' (13 March 1984) UN Doc CCPR/C/21/Add.3, para 4.

of individuals, or the electorate more broadly, to participate in the conduct of public affairs, including by choosing their political representatives through some kind of voting process.[139]

Finally, if the principle of non-intervention prohibits coercive interference in the *domaine réservé*, the concept of 'interference' deserves additional attention. The overwhelming majority of authors pay no attention to this criterion separately, but consume it under the heading of coercion – either the act is 'calculated to impose certain conduct or consequences on that other state' and it is 'of a certain magnitude' (coercive, thus intervention) or it is not (not coercive, thus no intervention).[140] The problem with this approach is that it is arguably over- and underinclusive at the same time. Overinclusive, because the connection between the act of the 'intervening' State and the exclusive domestic jurisdiction of the 'target' State is stretched to a breaking point. Almost any act carried out by a State on the international plane in some way 'affects' or 'bears on' matters in which another is permitted to decide freely[141] – even if the latter is interpreted restrictively (as it should).[142] Underinclusive, due to the combination of a near-insurmountable threshold for coercion (forcible or dictatorial interference only) and its highly contested nature beyond that (threats or attempts to coercively interfere, economic coercion[143]). In addition, the principle of non-intervention contributes very little in the case of *forcible* interference, as the more prominent prohibition on the use of force (Article 2(4) of the UN Charter) outlaws that independently.[144] Consequently, the *classical* two-fold test is hardly ever met: Almost all acts pass the first prong while almost all either fail the second or fall foul of Article 2(4). It is no wonder that this has led some to suggest that '[t]he most interesting question regarding the principle of nonintervention … is why on earth anyone should suppose that it exists'.[145]

A better approach takes all elements of non-intervention seriously, including 'interference'. In the context of VIOPS, that implies, first, that State A interfered with the *exercise* of State B and its people's right to choose their government. Second, interference denotes an activity that frustrates or hinders the exercise of that right – or, in the words of the ILC, makes it more difficult or onerous[146] – which, after all, has to remain free. Such an interpretation not only flows

---

[139] UN Human Rights Committee, 'The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service (General Comment 25)' (27 August 1996) UN Doc CCPR/C/21/Rev.1/Add.7, paras 2 and 6ff.

[140] Jennings and Watts (n 70) para 129, 430; Jamnejad and Wood (n 129) 348.

[141] Indeed, States even complain of 'interference' when they receive criticism on domestic policy from other States. For example, China has consistently denounced critique over its handling of the crisis in Hong Kong as blatant interference in its internal affairs. See opposing statements in the UN's Third Committee: (excerpts in) S Tiezzi, 'Which Countries Support China on Hong Kong's National Security Law' (9 October 2020) <https://thediplomat.com/2020/10/which-countries-support-china-on-hong-kongs-national-security-law/> and Germany, Permanent Mission to the United Nations, 'Statement by Ambassador Christoph Heusgen on behalf of 39 Countries' (6 October 2020) <https://new-york-un.diplo.de/un-en/news-corner/201006-heusgen-china/2402648>. Similarly, India denounced China for raising the issue of Kashmir as 'interference in [its] internal affairs': 'Kashmir: After China's Third Call for UNSC Meeting, India Rejects "Interference" *The Wire* (6 August 2020) <https://thewire.in/diplomacy/china-unsc-kashmir-meeting-india-reject-internal-matters-interfernce>.

[142] Jennings and Watts (n 70) para 129, 430; Jamnejad and Wood (n 129) 348. See also (n 121).

[143] See text accompanying (n 122-134). On economic coercion, see: Tzanakopoulos (n 127); Jamnejad and Wood (n 129) 369-72; ICJ *Nicaragua* case (n 67) paras 244-5.

[144] Not only does that include the direct use of force, it encompasses the arming and training of – but not the mere supply of funds to – rebel forces abroad also (ICJ *Nicaragua* case (n 67) para 228).

[145] V Lowe, 'The Principle of Non-Intervention: Use of Force' in C Warbrick and V Lowe (eds), *The United Nations and the Principles of International Law: Essays in Memory of Michael Akehurst* (Routledge 1994) 67.

[146] See text accompanying (n 127).

from the term's ordinary meaning,[147] but is further supported by human rights jurisprudence. For example, the European Court of Human Rights (ECtHR) has found interference in the exercise of the right to vote in cases where a person or group of persons were *disqualified* from doing so. Similarly, in the context of the right to freedom of thought, conscience and religion, the Court qualified as interference *inter alia* a criminal or administrative penalty, a physical obstacle (such as the interruption of a meeting) and the dissolution of a religious organization. Conversely, legislation which was 'generally and neutrally applicable in the public sphere' did not constitute interference with such freedoms.[148] In other words: Interference denotes State action that actually puts up barriers that complicate the free exercise of a right. Arguably, this is fully supported by the view expressed by New Zealand: A cyberoperation that '*deprives* a significant part of the electorate of the *ability to vote*' violates the non-intervention principle.[149]

The question thus becomes whether the Russian actions under examination – i.e., the social media campaign, the doxfare and(/or) the targeting of election infrastructure – meet a threefold test: (1) Does the action relate to a right in another State's *domaine réservé*? (2) Does the action interfere with the free exercise of such a right? (3) Does the action employ methods of coercion? If and only if, the answer to all three questions is yes, a violation of the non-intervention principle has occurred. However, it is submitted that while the three actions under review certainly relate to the right of a State and its people to choose their political leadership – a right that clearly belongs to a State's *domaine réservé*[150] – they did not (and could not) effectively interfere with the exercise of that choice.[151]

This is true because not a single American voter was frustrated or hindered in casting a ballot in good conscience. Indeed, how could they have been since most of the acts complained of involved the mere transmission of news or propaganda (true, false or a combination of the two)? So while one can argue that there was Russian *involvement* in the election process, they would be much harder-pressed to claim Russian *interference* with the right to vote of even a single citizen, let alone the electorate more broadly. And even if we were to accept that individual voters' right to hold an opinion was affected (*quod non*), as the basis for the free formation and expression of a political preference, that interference could still not be said to have used methods of coercion.[152]

---

[147] See <https://www.merriam-webster.com/dictionary/interfering>. See also, e.g., Schmitt (n 8) 45.

[148] ECtHR, 'Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights' (Updated on 31 August 2020) <https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf> 8-13; ECtHR, 'Guide on Article 9 of the European Convention on Human Rights' (Updated on 31 August 2020) <https://www.echr.coe.int/Documents/Guide_Art_9_ENG.pdf> 16-17. See also: W Schabas, *The European Convention on Human Rights: A Commentary* (OUP 2015) 402-6 and the thought-provoking (pun intended) work of Judith Vermeulen (UGent), for example in 'Recommended for You: "You Don't Need No Thought Countrol". An Analysis of News Personalisation in Light of Article 22 GDPR' in M Friedewald et al, *Privacy and Identity Management. Data for Better Living: AI and Privacy* (Springer 2019) 194-8.

[149] New Zealand (n 43) (emphasis added).

[150] See text accompanying (n 114-120). See also: Sander (n 8) 21.

[151] To be fair, this is a different question than that of whether the VIOPS have had any real impact, on which this article does not take a position. But compare: Y Benkler, 'The Danger of Overstating the Impact of Information Operations' (*Just Security*, 23 October 2020) <https://www.lawfareblog.com/danger-overstating-impact-information-operations> with that taken by Jamieson in *Cyber-War: How Russian Hackers and Trolls Helped Elect a President* (OUP 2018).

[152] See, for example, M Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (2nd edn, Engel 1993) 442. Others, such as Wheatley ('Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-intervention' (*EJIL:Talk!*, 26 October 2020) <https://www.ejiltalk.org/cyber-and-influence-operations-targeting-elections-back-to-the-principle-of-non-intervention/>), disagree and

The difference between the alleged Russian involvement in the US election and true interference with the right to vote becomes even clearer through a comparison with the century-old, State-sanctioned voter suppression effort in the United States. According to the American Civil Liberties Union (ACLU), politicians are passing measures all over the US making it harder to cast a ballot:

> Suppression efforts range from the seemingly unobstructive, like voter ID laws and cuts to early voting, to mass purges of voter rolls and systemic disenfranchisement. … [L]egislators can redraw district lines that determine the weight of your vote. Certain communities are particularly susceptible to suppression and in some cases, outright targeted — people of color, students, the elderly, and people with disabilities.[153]

The net result is that according to the Perceptions of Electoral Integrity dataset – an independent academic project based at Harvard University and drawn from a rolling survey of 3,861 expert assessments of electoral integrity across 337 elections in 166 countries around the world – the US ranks second to last among the world's liberal democracies, leaving only Albania behind it.[154] Therefore, even if we take all allegations made about Russian cyberoperations as fact, they are clearly of a different nature than, and pale in comparison to, the interference unleashed by elected US officials against their own citizens.

More importantly for the purposes of this article, it clarifies what real interference looks like and why Russian activities – at least those documented in Section 2 and, again, if taken as fact – simply do not meet the legal threshold. Indeed, even if the election infrastructure was breached and sensitive voter data was obtained,[155] that would not automatically result in a violation of international law – at least not if the 'conservative' view of sovereignty in cyberspace is adopted.[156] However, should Russia succeed in hitting with ransomware infrastructure that certifies tallies, vulnerable voter registration systems or electronic poll books, which recent media reports suggest are unfolding,[157] the legal assessment could well shift dramatically.

---

claim that 'there are circumstances when lying is the functional equivalent of coercion'. He provides the example of releasing a 'deep fake' video during an election process showing candidates saying or doing something they never said or did; or false reports of an active shooter situation to suppress voter turndown. According to Wheatley, the electorate would be coerced: it 'will have been given no meaningful choice in the matter, because they now have a false perception of the true facts of the situation, which formed the basis on which they cast their votes'. In this context, see also: B Baade, 'Fake News and International Law' (2019) 29 EJIL 1357, 1362-5. However, and blowing past the difficulty of defining 'truthful' information, it remains utterly unclear *when, exactly* a fake news item would succeed in abolishing meaningful choice for an individual voter given that surely not every lie – no matter how small, insignificant or implausible – covertly pushed by third States can be thought to achieve such a result. In addition, such an outcome-based approach appears to again present target States with a no-win scenario – either discover and debunk the lie (well-informed electorate, but no intervention) or overlook it and suffer the consequences (misinformed electorate, but intervention) – while providing the wrong incentive for rogue States.

[153] For a helpful overview, see: ACLU, 'Block the Vote: Voter Suppression in 2020' (3 February 2020) <https://www.aclu.org/news/civil-liberties/block-the-vote-voter-suppression-in-2020/> and C Anderson, 'The Five Ways Republicans Will Crack Down on Voting Rights in 2020' *The Guardian* (13 November 2019) <https://www.theguardian.com/us-news/2019/nov/13/voter-suppression-2020-democracy-america>. For an excellent documentary, see Liz Garbus and Lisa Cortes' *All In: The Fight for Democracy* (2020) <https://www.allinforvoting.com/>.

[154] P Norris and M Grömping, Electoral Integrity Project, 'Electoral Integrity Worldwide' (May 2019) <https://www.electoralintegrityproject.com/the-year-in-elections-2017>.

[155] See text accompanying (n 26-29 and 60-63).

[156] See Section 3.1.

[157] See, for example: D Sanger and N Perlroth, 'Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing the Same, *The New York Times* (12 October 2020) <https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html>.

Finally, we should compare this position on VIOPS and non-intervention with that taken by other scholars under this same heading. The generally accepted understanding, exemplified by the Interactive Cyber Toolkit's summary, is that such operations 'targeted against the electorate in State A … would likely not reach the level of coercion and, as such, would not amount to prohibited intervention'. The generally accepted exception to that rule is a scenario whereby the election results would in fact be manipulated, for example through tampering with the electronic ballot system, as it would coercively 'deprive State A of the ability to choose its political representatives on the basis of the free expression of the will of the electorate'.[158] This is further echoed by the *opinio juris* of multiple States.[159] Many commentators therefore seem to agree on certain paradigmatic examples where a VIOPS breaches the non-intervention principle, even if the argumentative route they take may vary significantly.

Alternatively, there are plenty of scholars that take a more expansive view for example by espousing the notion that the covert element of disinformation distinguishes it from (lawful) overt propaganda or 'mere' influence operations. It could then be argued that the influencing State 'by implication is seeking to compel an outcome' because of the 'inability of the target state to maintain an open democratic space in which to conduct free and fair elections'.[160] On that basis, such State behaviour may also be considered coercive and consequently falls foul of the non-intervention principle. However, it is entirely unclear what (primary) sources of international law support this view that equates deception to coercion – a point readily conceded by its proponents.[161] Ultimately, it is difficult to see how creating a situation in which the American electorate 'could not fairly evaluate the information it was being provided' because of the 'covert nature of the troll operation' could ever make casting a ballot for the next US President more difficult or onerous for even a single voter. There appears to be no interference with that right – let alone one that reaches the required level of coercion. For that reason, this interpretation should be discarded.

There are other thought-provoking interpretations that nevertheless fail to convince. For example, Forcese and Koh both invoke a statement of the first edition of the Tallinn Manual, which determined that 'manipulation by cyber means of … public opinion on the eve of elections, as when online news services are altered in favour of a particular party, false news is spread, or the online services of one party are shut off' might very well constitute coercive political interference and a violation of the non-intervention principle.[162] That understanding is moreover (albeit exclusively)

---

[158] Interactive Cyber Toolkit (n 8) Scenario 01: Election interference. See also: Crootof (n 8) 628-31.
[159] See Section 2.2.
[160] Moynihan (n 8) 41-2; Schmitt ((n 8) 51). See also: M Schmitt, 'Foreign Cyber Interference in Elections: An International Law Primer' Part I-III (*EJIL:Talk!*, 16 October 2020) <https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-i/>; Helal (n 8) 114-15; Sander (n 8) 21-4.
[161] For example, and to his credit, Schmitt ((n 8) 52-3) admits that 'a significant grey zone lies between the easy cases' that either clearly breach a meddling State's obligations or not – a grey zone that 'creates legal uncertainly and affords States fertile ground in which to meddle in each other's political activities'. Or see Kilovaty ((n 8) 179) who seeks to expand intervention to include disruptive yet not coercive doxfare. His is, however, clearly an argument *de lege ferenda*. Similarly, Hollis (n 8) argues for a prohibition that bans non-coercive interference. In the same vein, Barela (n 8) admits his threshold of coercion diverges from a strict doctrinal interpretation. While those may very well be laudable policy proposals, by their own admission they do not accurately represent the law as it stands today. But see: Wheatley (n 152).
[162] Forcese (n 8); Koh (n 8) 450-1. See also: Schmitt, 'Foreign Cyber Interference in Elections: Part I' (n 160).

backed by Iran.[163] However, the statement was not retained in the Tallinn Manual 2.0, indicating a significant loss of support by its authors. Arguably, the position also raises more questions than it answers, thereby failing to bring legal clarity to an already obfuscated debate.

A final argument to be assessed, yet ultimately rejected, is one most prominently adopted by Jens David Ohlin and relies heavily on the right to self-determination. According to him,

> there are a class of procedural rules that are so fundamental that without them, an election cannot be said to express the popular will. These procedural rules are 'boundary' rules, rules that distinguish between insiders and outsiders, between citizen participation and foreign participation, both with regard to voting but also spending and electioneering. *When elections involve substantial foreign participation, the result of the election no longer expresses the will of the people, but a mixture of that will combined with the will of the foreigners who have infiltrated the election.* This type of election interference violates the collective right of self-determination.[164]

He moreover lays out and refutes four objections offered by international lawyers against that interpretation: self-determination applies before statehood but not after, there is insufficient State practice or *opinio juris* to support the theory, there is too much contradictory State practice and, finally, self-determination does not apply extra-territorially.[165]

However, there is a more potent fifth objection – or, if you will, a spin on the first one – that accepts the continuation of the (collective) right to self-determination even after a people has attained its independence in a new State albeit that the protection it offers against third-State interference is then provided by the principle of non-intervention. As noted above, Crawford probably formulated it best: '[i]n this case the principle of self-determination normally takes the well-known form of the rule preventing intervention in the internal affairs of a State'.[166] Rather than viewing self-determination as a *separate* rule of international law protecting against third-State interference, it is inextricably linked with the principle of non-intervention so that they should be treated in tandem (as in this section) and it is the latter that sets the accurate legal standard to assess the legality *vel non* of election meddling.[167]

In the end, this article agrees with Keitner who astutely noted that 'States appear by and large to have maintained a posture of constructive ambiguity when it comes to the international lawfulness of influence operations—via cyber

---

[163] Iran (n 44).
[164] Ohlin (n 8) 116. But see: Schmitt, 'Foreign Cyber Interference in Elections: Part I' (n 160): 'The argument is facially plausible, but this interpretation of the right presents numerous challenges.'
[165] ibid 108-16.
[166] Crawford (n 117). This view that ties together both norms seems to be supported by Tsagourias (n 8), who nevertheless then reinterprets coercion in that context as control: 'such operations … are purposively designed to exert control over a sovereign matter … through subterfuge for example false, fabricated, misleading, or generally manipulated information.' In that way, he falls in the category of Moynihan, Schmitt and Helal whose views have been challenged above (see text accompanying (n 160-161)). See also Lahmann (n 8): '[T]he state's sovereignty acts as a mediator of the people's self-determination and must be interpreted accordingly. It functions as a shield against certain forms of outside interference – deceptive, manipulative conduct – and thus safeguards both the state itself and its people's right to free decision making.' As explained above, this view cannot hold.
[167] See explanation provided in text accompanying (n 114-117).

means or otherwise—that do not directly alter votes as they were cast'.[168] Barring some clear-cut cases, these actions indeed take place in a grey area – but the logical consequence thereof is that they are simply not (yet) prohibited by international law.[169]

4 Conclusion

Few commentators would disagree that a State-sanctioned policy designed to sway the results of an election process abroad, through influence operations of the foreign electorate, constitutes unfriendly or even malign inter-State behaviour. While such behaviour is by no means exceptional from a historical point of view, international lawyers sat up and took special notice after Russian VIOPS contributed to the election of Donald Trump as the next 'leader of the free world', who was and remains less than popular among large swaths of the population in the United States and across the globe – to put it mildly.[170]

However, that does not *ipso facto* mean that such nefarious actions are unlawful under international law. Indeed, this article's modest aim was to examine if and under what circumstances voter influence operations in cyberspace violate the principle of sovereign equality and the principle of non-intervention (read in conjunction with the right to self-determination). For both cardinal rules of international law, the often-overlooked concept of 'interference' appears to play a pivotal role. First, a State-sanctioned cyberact constitutes a sovereignty violation if it either directly interferes with another State's territorial integrity (damage or injury to, or the serious loss of functionality of, election infrastructure) or inherently governmental functions (such as the conduct of elections). Additionally, or alternatively, when such an act coercively interferes with a foreign electorate's right to vote it breaches the principle of non-intervention. However, if it meets neither of these thresholds, as appears to be the case for most examples of information manipulation and cyber disruption, neither rule of international law is violated. To sum up: No interference? No problem!

However, none of that should result in a defeatist attitude. If States decide this kind of behaviour is no longer acceptable, they have several options at their disposal. First, they can adopt domestic legislation prohibiting such behaviour on their territory – as many, including the United States, have done.[171] Second, they can take up Russian President Vladimir Putin's offer to negotiate an all-encompassing international treaty on cyberspace, opt to revamp the aforementioned UNGA resolutions that seem to have died a quiet death, or redouble their efforts in promoting the work of the abovementioned inter-State fora (some under the auspices of the United Nations). Third, a simple

---

[168] Keitner (n 8) 19.
[169] PCIJ *Lotus* case (n 66) 18.
[170] 'How Popular is Donald Trump?' (*FiveThirtyEight*, updated on 24 October 2020) <https://projects.fivethirtyeight.com/trump-approval-ratings/>; R Wilke et al, 'Trump Ratings Remain Low Around Globe, While Views of U.S. Stay Mostly Favorable' (*Pew Research Center*, 8 January 2020) <https://www.pewresearch.org/global/2020/01/08/trump-ratings-remain-low-around-globe-while-views-of-u-s-stay-mostly-favorable/>.
[171] For just one example, on domestic legislation regulating political finance (including from foreign interests), see: Institute for Democracy and Electoral Assistance, 'Political Finance Database' (2020) <https://www.idea.int/data-tools/data/political-finance-database>.

majority of states (present and voting) at the UNGA can request an ICJ Advisory Opinion, wherein the Court could put to rest remaining legal controversies on the topic.

In the end, Tzanakopoulos formulates it well when commenting on another aspect of the 'fundamental right' to be free from foreign interference:

> Politics can establish fundamental rights of states as a legal category; political struggle can change the law. And the people can change politics, even if with great difficulty. But in the meantime, labouring under the illusion that the law poses some outer limit to evil … merely deflects our energy from where it is needed: political activism and political struggle. … Do you want there to be a fundamental right of states to be free from economic coercion? Splendid! Go out there and make one.[172]

That quote applies equally beautifully to voter influence operations and international law.

[172] Tzanakopoulos (n 127) 633.