University of St. Thomas Journal of Law and Public Policy

Volume 15
Issue 2 *Alternate Realities: Conspiracy Theory and the Constitutional and Democratic Order*

Article 29

April 2022

An International Law Perspective on Political Informational Warfare: The Challenges of Combating the Weaponized Use of Conspiracy Theories and Disinformation to Undermined Democracy

Kimberly Breedon

AN INTERNATIONAL LAW PERSPECTIVE ON POLITICAL INFORMATIONAL WARFARE: THE CHALLENGES OF COMBATING THE WEAPONIZED USE OF CONSPIRACY THEORIES AND DISINFORMATION TO UNDERMINE DEMOCRACY

KIMBERLY BREEDON*

I. INTRODUCTION

Illiberal authoritarian regimes have in recent years employed increasingly effective online disinformation, conspiracy theory, and other psychological influence campaigns designed to manipulate voter opinion-making and political outcomes in democratic societies.[1] Disturbingly, domestic public officials in democratic societies are also increasingly joining or even initiating such informational warfare[2] campaigns against their own citizens. In this environment, the implications for international law development merit scrutiny.

One issue warranting attention is how the role of domestic political actors in advancing disinformation campaigns and other tools of informational warfare may undermine the consent requirement of the sovereignty principle and may implicate the coercion element of the non-intervention principle of international law. In other words, when a target State's complicit governmental actors perpetuate disinformation campaigns,

---

* Assistant Professor of Law, Ohio Northern University College of Law. Author's note: A heartfelt thanks to Julianna Burchett and Ellaheh Sims for their excellent research assistance; to the participants of the University of St. Thomas School of Law Journal of Law & Public Policy Spring Symposium: Alternative Realities, Conspiracy Theory, and the Constitutional and Democratic Order for their insights and perspectives; and to Mark Summers for his helpful comments and suggestions on an earlier draft of this paper. All errors, of course, are mine.

[1] *See, e.g.*, CATHERINE A. THEOHARY, CONG. RSCH. SERV., R45142, INFORMATION WARFARE: ISSUES FOR CONGRESS (2018); EDWARD LUCAS & PETER POMERANZEV, CTR EUR. POL'Y ANALYSIS, REPORT, WINNING THE INFORMATION WAR: TECHNIQUES AND COUNTER-STRATEGIES TO RUSSIAN PROPAGANDA IN CENTRAL AND EASTERN EUROPE (2016), https://cepa.org/cepa_files/2016-CEPA-report-Winning_the_Information_War.pdf; OFF. DIR. NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY (2021).

[2] *See infra*, Part I.B, C.

thereby tacitly allowing, explicitly encouraging, or even actively facilitating, intervention by a foreign State in the target State's democratic opinion-making, does the conduct by domestic actors operate to circumvent a foreign State's duty of non-intervention without the target State's consent, as applied to online operations seeking to manipulate voting behavior? This Article examines some of the difficulties posed by the present international legal framework in answering that question. First, however, a brief caveat: the purpose and scope of this Article are limited to identifying some of the relevant questions for further research relating to the weaponization of conspiracy theories and disinformation to manipulate democratic decision-making, and to sketching out under-theorized corollary considerations relating to the development of customary international law as to information warfare. This Article does not offer a complete survey of the current state of affairs in this area, nor does it propose analytical solutions to the issues identified. The goal, rather, is to shine a light on, and to prompt discussion of, these issues.

The discussion proceeds as follows. Part I introduces the problem, including examples of past and apparently ongoing disinformation and conspiracy theory campaigns initiated or amplified both by authoritarian regimes targeting democratic opinion-making in other states and by domestic political officials and their proxies. Specifically, Part I will briefly explore relevant events in Estonia, Poland, and the United States.

Part II reviews relevant international law principles, including both the background and the current status of those principles as applied to online operations targeting voter opinion-making and political preferences. More particularly, Part II will discuss the international law principles of sovereignty and non-intervention, including the discrete aspects of those rules that may create difficulties for customary international law development when target states facilitate a foreign state's information warfare by remaining silent. In addition, Part II considers the principle of self-determination as an alternative, if unconventional, basis for holding infringing governments accountable for interference with a target state's democratic opinion-making.

Part III explains the need for clarity on the application of international rules as applied to cyber-based activities and discusses the difficulties that states' silence poses for the development of customary international law in this area. Part IV then examines some of the challenges that arise in the application of the international law principles to cyberspace when complicit or aligned domestic government heads are either involved in

perpetuating the same conspiracy theories or disinformation campaigns as those propagated by a foreign government seeking to manipulate the democratic opinion-making in the target State or when those domestic government heads are silent in the face of such activities and that silence has been corruptly or coercively secured by the foreign State. Finally, Part V offers a brief conclusion.

II. EXAMPLES OF CONSPIRACY THEORIES AND DISINFORMATION CAMPAIGNS TARGETING DEMOCRATIC OPINION MAKING

To contextualize the issues which may arise under international law relating to a foreign State's cyber-based activities that use conspiracy theories and disinformation campaigns to manipulate the democratic opinion-making of another State, under circumstances in which the target State fails to object to, or seeks to counter, such campaigns, this Part provides examples of two categories of information warfare campaigns: (1) the weaponized use of such campaigns by political leaders against their own citizens; and (2) the weaponized use of such campaigns by a State against the population of another State. The first category demonstrates that the government leader of a State which is the target of a foreign State's cyber operations that propagate and amplify conspiracy theories and disinformation campaigns may be willing to accept those operations if they prove politically or personally beneficial to him or her. The second category demonstrates that these sorts of campaigns, sometimes called "hostile measures," present ongoing threats to democratic governance.

First, however, it is worth pausing for a moment to consider the goals of foreign governments in conducting cyber operations of this type. In this regard, Russia is representative. Although by no means the only government to employ such tactics,[3] Russia, which has a long history of using hostile measures to advance its interests,[4] presents a particularly aggressive and

---

[3] Marisa Endicott, *Propaganda's New Goals: Create Confusion, Sow Doubt,* U.S. NEWS & WORLD REP., Jan. 31, 2017, https://www.usnews.com/news/national-news/articles/2017-01-31/russian-propagandas-new-goals-create-confusion-sow-doubt ("The Kremlin is not alone in pushing disinformation campaigns. Propaganda from the Islamic State group (also known as ISIS), Israel and China abounds...").

[4] STEPHANIE YOUNG & BRENNA ALLEN, RAND CORP., RUSSIA'S HOSTILE MEASURES: COMBATING RUSSIAN GRAY ZONE AGGRESSION AGAINST NATO IN THE CONTACT, BLUNT, AND SURGE LAYERS OF COMPETITION APP. A 77 (2020); LUCAS & POMERANZEV, *supra* note 1, at 11; Endicott, *supra* note 3 ("Russia's propaganda efforts are well-established, dating back through the Cold War and Soviet era all the way to the Russian Revolution in 1917.").

successful example, having employed various measures against multiple countries targeting vulnerabilities across myriad sectors.[5] Among other examples of hostile measures that Russia has used in the past dozen or so years, the most salient for purposes of this Article are intervening in the domestic political movements in target states and launching disinformation campaigns directed at target states' polities.[6] Russia, like other illiberal regimes, uses hostile measures, such as cyber-attacks and disinformation campaigns to achieve specific objectives with one long-term goal: weakening and dismantling liberal western democracies.[7] According to a report published in April 2021 by the United States Office of the Director of National Intelligence, the specific objectives used to achieve this goal are illustrated by Russia's information warfare against the United States and include the following: undermining the position of the United States as a global leader, sowing internal discord, influencing American voters, and shaping decision-making by the U.S. government.[8] In addition, such operations aim to create doubt about the legitimacy of electoral outcomes[9] and to undermine the stability and security of western democratic alliances.[10]

---

[5] STEPHANIE PEZARD, ET AL., RAND CORP., RUSSIA'S HOSTILE MEASURES: COMBATING RUSSIAN GRAY ZONE AGGRESSION AGAINST NATO IN THE CONTACT, BLUNT, AND SURGE LAYERS OF COMPETITION APP. B (2020).

[6] *Id.*; OFF. DIR. NAT'L INTEL., *supra* note 1, at 11 ("Russia presents one of the most serious intelligence threats to the United States...influencing US voters and decisionmaking. Russia will continue to advance its technical collection and surveillance capabilities and probably will share its technology and expertise with other . . . US adversaries.").

[7] "A democracy is only as resilient as its people. An informed and engaged citizenry is the fundamental requirement for a free and resilient nation.... Today, actors such as Russia are using information tools in an attempt to undermine the legitimacy of democracies. Adversaries target media, political processes, financial networks, and personal data." THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 14 (Dec. 2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[8] OFF. DIR. NAT'L INTEL., *supra* note 1, at 11 ("Moscow almost certainly views US elections as an opportunity to try to undermine US global standing, sow discord inside the United States, influence US decisionmaking, and sway US voters. Moscow conducted influence operations against US elections in 2016, 2018, and 2020."). *See also* Steven J. Barela, *Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion*, JUST SECURITY, Jan. 12, 2017, https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion.

[9] Barela, *supra* note 8.

[10] BEN CONNABLE, ET AL., RAND CORP., RUSSIA'S HOSTILE MEASURES: COMBATING RUSSIAN GRAY ZONE AGGRESSION AGAINST NATO IN THE CONTACT, BLUNT, AND SURGE LAYERS OF COMPETITION, at iii (2020).

Given these objectives, the particulars of information warfare campaigns tend to be tailored to the specific circumstances of the State where they are employed.[11] Some examples will illustrate. The following subsections discuss information warfare campaigns aimed at the democratic opinion-making of, respectively, Estonia, Poland, and the United States.

A. Estonia – The Bronze Soldier

Soon after the tiny Baltic country of Estonia joined the European Union and the North American Treaty Organization in 2004, Russia intensified an ongoing campaign to exacerbate tensions and divisions between the nation's ethnic Russian minority,[12] which accounts for approximately 25% of the population, and its Estonian majority.[13] The focus for this effort eventually, and effectively, centered on a statue located in a park in the center of the capitol city, Tallinn: The Bronze Soldier.[14] Erected during the Soviet Union's occupation of Estonia after World War II, ostensibly as a monument to honor the fallen soldiers of the Red Army in their fight to "liberate" Estonia from Nazi Germany,[15] the statue became a symbol of the divisions between ethnic Russian Estonians and the non-Russian majority in the post-independence era.[16]

The Kremlin, recognizing and capitalizing on these tensions, has used them as the basis for its information warfare campaign against Estonia

---

[11] Endicott, *supra* note 3 ("Russian disinformation . . . targets different communities using different languages in countries all over the world with messages and methods uniquely tailored to each audience.").

[12] LUCAS & POMERANZEV, *supra* note 1, at 21.

[13] Stefan Meister, et al., Institute für Auslandsbeziehungen, *Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia*, IFA EDITION CULTURE & FOREIGN POL'Y 33 (2018), https://nbn-resolving.org/urn:nbn:de:0168-ssoar-59979-0.

[14] NINA JANKOWICZ, HOW TO LOSE THE INFORMATION WAR: RUSSIA, FAKE NEWS, AND THE FUTURE OF CONFLICT 21, 24-34 (2020) (The formal title of the statue is the Soviet Monument to the Liberators of Tallinn.); Meister, et al., *supra* note 13.

[15] JANKOWICZ, *supra* note 14, at 24-25.

[16] Francis Tapon, *The Bronze Soldier Explains Why Estonia Prepares for A Russian Cyberattack*, FORBES, July 7, 2018, https://www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/?sh=607f9c98c7a0 ("For many Estonians, the Bronze Soldier represents 48 years of Soviet oppression. Meanwhile, Russians believe that the statue represents the triumph over the Nazis.").

to perpetuate "the perception of a growing anti-Russian movement" there.[17] As is often the case with effective disinformation, this narrative contained some truth to it. The source of Estonia's ethnic divisions is deeply rooted. Russians who lived in Estonia when it regained its independence in 1991 were subjected to newly enacted citizenship laws that required proficiency in the Estonian language. Those unable to meet the language requirements were denied not only Estonian citizenship, but also access to certain public services, including public education. Disparities between ethnic Russians and Estonians continued, and the discontent of the Russian-speaking minority grew.[18]

For its part, during the early 2000's, shortly after Vladimir Putin became Russia's President, the Kremlin sought to reinforce Russian-Estonians' cultural and linguistic ties to Russia by implementing a strategy to rally the Russian diaspora in Estonia around Soviet symbols and celebrations of "Victory Day"—the date commemorating the Soviet Union's declaration of victory over Nazi Germany.[19] Accordingly, as Russian-Estonians became increasingly dissatisfied with their disparate treatment by the Estonian government, and as the Kremlin targeted them with propaganda campaigns, both to stoke divisions internally and to draw ethnically Russian-Estonians closer to Russia, the size of the Victory Day celebrations increased by the year, and the Bronze Soldier "[became] an increasingly significant symbol of unity for ethnic Russians."[20] It also served as the flashpoint for "the worst civil unrest" in post-independence Estonia: an overnight period of rioting in April 2007, known as the "Bronze Night."[21]

Though culminating on the Bronze Night, conflict involving the Bronze Soldier had long been simmering. In 2005, members of Nashi, a Russian nationalist youth organization funded by the Kremlin, began participating in the Victory Day celebrations near the statue.[22] At a 2006 Victory Day observance, a group of Estonian nationals carrying the Estonian

---

[17] Meister, et. al., *supra* note 13 (Among Russia's broader objectives that it sought to achieve by conducting this information warfare campaign was to weaken support for Estonia from its international allies, especially its western democratic allies in Europe and the United States, by creating the perception that the Estonian population consisted of "closet Nazis" who were "xenophobic, intolerant, and hostile."); LUCAS & POMERANZEV, *supra* note 1, at 21.

[18] JANKOWICZ, *supra* note 14, at 25.

[19] *Id.* at 26-27; LUCAS & POMERANZEV, *supra* note 1, at 22.

[20] LUCAS & POMERANZEV, *supra* note 1, at 22.

[21] *Id.* at 22-23.

[22] JANKOWICZ, *supra* note 14, at 30.

flag made a counter-appearance in response to the ethnic Russian celebrations.[23] Because the Estonian group was significantly smaller, and because the situation was volatile, the Estonian police, fearing violent confrontations between the two sides, removed the Estonian group.[24] At some point during the 2006 Victory Day celebration, an Estonian flag was torn down.[25]

In response to the growing tensions and in the aftermath of the 2006 Victory Day conflict, as the Estonian government debated whether to move the Bronze Statue from its central location in the capital to a military cemetery on the edge of town,[26] a group of ethnic Russians, with the aid of the Russian Embassy in Estonia, formed the "Nochnoi Dozor" (translated into English as "Night Watch"),[27] an organization with the self-appointed task of guarding the monument during the overnight hours from any efforts the Estonian government might take to dismantle and relocate it at nighttime.[28]

Meanwhile, rumors proliferated about what may lay buried beneath the monument. According to one report, speculation ran the gamut about what the site interred—from deceased patients from a nearby hospital to executed criminals to inebriated Soviet soldiers whose own tanks had run over them.[29] By April 2007, the Estonian government had decided to excavate the site to ascertain what, if anything, had been buried there to be able to relocate "the monument and any remains...honorably and properly."[30] The excavation began, out of public view behind a fence and tent, on the morning of April 26.[31] As the day progressed—after weeks of anti-Estonian propaganda in Russian media, including accusations that the Estonian government was "attempting to destroy the memorial and desecrate the

---

[23] *Id.* at 31.

[24] *Id.*

[25] LUCAS & POMERANZEV, *supra* note 1, at 22.

[26] *Id.*; *see also* Meister, et al., *supra* note 13, at 32.

[27] LUCAS & POMERANZEV, *supra* note 1, at 22.

[28] JANKOWICZ, *supra* note 14, at 32; *see also* Meister, et al., *supra* note 13, at 32 (noting that the Nochnoi Dozor "took an active role in protecting the monument") (The Estonian Internal Security Service has attributed the formation of the Nochnoi Dozor to Russian intelligence figures and believes that the Russian Federal Security Service (the FSB) is responsible for coordinating a number of operations relating to the Bronze Soldier, including the spread of propaganda and disinformation.); LUCAS & POMERANZEV, *supra* note 1, at 22-24.

[29] Tapon, *supra* note 16.

[30] JANKOWICZ, *supra* note 14, at 33.

[31] *Id.*

memory of Russian soldiers who fought the Nazis"—hundreds of people gathered at the site.[32] By early evening, rioting had begun.[33] Throughout the night and into the next day, rioters clashed with law enforcement, attacked public buildings, and destroyed private property.[34] Against this backdrop, during the early morning hours of April 27, the Estonian government decided to relocate the statue immediately, even as the rioting continued.[35] Within only a few hours of that decision, the monument had been removed.[36]

The events leading up to and including the Bronze Night were accompanied by the steady drumbeat of Russian propaganda and disinformation. Indeed, according to a report by the Center for European Policy and Analysis, the Bronze Night "was an excellent example of a carefully prepared and executed Russian disinformation campaign...."[37] After the removal of the Bronze Statue, however, the disinformation efforts kicked into high gear. Russian state media is the primary source of information for Russian-Estonians, and even before the Bronze Night, Russian outlets presented the prospect of the monument's removal as "an attack against Russia's cultural values, the Russian language, human rights, religious beliefs and the nation's sacred origins."[38] As the events of the Bronze Night unfolded, and in the days that followed, Russian media blended video footage from Tallinn, which was sometimes staged or faked, with reports that relied on "distortions, half-truths, and outright lies."[39]

For a population primed to believe that the decision to move the Bronze Soldier was "a sinister assault on Russian culture,"[40] Russian-Estonians were all too prepared to believe the narratives supplied by Russian media, which, among other things, falsely described violent acts of vandalism by ethnically Russian youth gangs as peaceful demonstrations; asserted fabricated acts of police brutality; and lied that Estonian officials had cut the Bronze Soldier in half instead of relocating it.[41] In this stew of disinformation, additional conspiracy theories took root, including rumors that the remains of soldiers interred beneath the statue had been excavated

---

[32] LUCAS & POMERANZEV, *supra* note 1, at 23.
[33] JANKOWICZ, *supra* note 14, at 33.
[34] LUCAS & POMERANZEV, *supra* note 1, at 23.
[35] *Id.*
[36] JANKOWICZ, *supra* note 14, at 35.
[37] LUCAS & POMERANZEV, *supra* note 1, at 21.
[38] *Id.* at 22.
[39] *Id.* at 23.
[40] Endicott, *supra* note 3.
[41] LUCAS & POMERANZEV, *supra* note 1, at 23.

and discarded and that the Russian-Estonians who had tried to protect the statue had been tortured.[42] Fortunately for Estonia, the rioting was quashed relatively quickly, and the worst case scenario—entrenched political instability—was averted.[43] Equally significant, however, was Estonia's whole-of-government long-term response to the crisis, which has included a concerted effort both to counter Russian disinformation and to bridge disparities that for so long divided the country.[44]

The Estonian government's united efforts to fight Russian disinformation and to address the underlying societal rifts that make certain parts of its population susceptible to it stand in stark contrast to the willingness of Polish political leaders to weaponize conspiracy theories and disinformation for political gain.

B. Poland – The Smolensk Plane Crash

National tragedy struck Poland on April 10, 2010, when an airplane carrying Polish President Lech Kaczynski and nearly 100 high-level government officials crashed near the Russian town of Smolensk.[45] No one survived.[46] In the immediate aftermath of the disaster, Poles were united in their mourning of the devastating loss of life and leadership.[47] Unfortunately, however, the disaster that killed President Kaczynski and the delegation of government officials accompanying him also gave birth to a host of divisive conspiracy theories centering around the belief that Russia was responsible for deliberately downing the aircraft.[48] According to a nationwide poll conducted nearly a decade after the crash, at least 26% of Polish citizens wrongly believed that Russia had planned a coordinated attack on the plane, perhaps for the purpose of assassinating the President.[49] Russia, for its part, has been happy to witness the internal political turmoil caused by the plane crash, and though many of its actions, such as refusing to return the wreckage of the plane to Poland, have tended—perhaps intentionally—to fan the conspiracy-theory flame, Russia did not originate the disinformation

---

[42] *Id.*

[43] *Id.* at 23-24.

[44] JANKOWICZ, *supra* note 14, at 42-51.

[45] *Id.* at 87, 89; Monika Sieradzka, *Smolensk: The Tragedy that Defined Polish Politics*, DEUTSCHE WELLE, Apr. 10, 2018, https://www.dw.com/en/smolensk-the-tragedy-that-defined-polish-politics/a-43328611.

[46] JANKOWICZ, *supra* note 14, at 89; Sieradzka, *supra* note 45.

[47] JANKOWICZ, *supra* note 14, at 90; Sieradzka, *supra* note 45.

[48] JANKOWICZ, *supra* note 14, at 95; Sieradzka, *supra* note 45.

[49] JANKOWICZ, *supra* note 14, at 95; Sieradzka, *supra* note 45.

campaign;[50] Poland inflicted that particular wound on herself.[51] Fueling the conspiracy theories have been the political calculations of the leader of Poland's ruling Law and Justice Party (translated from the Polish *Prawo i Sprawedliwosc* and abbreviated as "PiS"), Jaroslaw Kaczynski, Lech Kaczynski's twin brother, who, despite having reportedly admitted to an aide that he did not believe the conspiracy theories, has not only declined to tamp them down, but instead has perpetuated them to gain political advantage.[52] Kaczynski even went so far as to accuse the opposition party of colluding with Russia to down the plane.[53]

Several official investigations conducted by both Poland and Russia concluded that human error, poor visibility, and the state of disrepair of the landing strip were the combined causes of the crash,[54] but even as the facts increasingly pointed to accidental causes, Kaczynski reaffirmed his public embrace of conspiracy theories, referring to the crash as "an unprecedented crime" and calling for a parliamentary investigation.[55] After prevailing in the 2015 election, winning the presidency and a parliamentary majority, the PiS government took several actions that operated to entrench a conspiracy theory as official policy: first, it "removed the original crash report from [the government's] website";[56] second, it "officially reopened the investigation into the crash";[57] third, it "created a new commission to explore [the] causes [of the crash]";[58] finally, and ghoulishly, it "exhumed crash victims, searching for traces of explosives on their bodies."[59] The effects of propagating conspiracy theories in service of the PiS's political machinations have been to polarize Polish voters, causing the nation to focus its attentions inwardly, and to diminish Poland's standing among its western allies—all

---

[50] In Poland's case, Russia did not launch cyber operations creating or amplifyi ng conspiracy theories or disinformation campaigns. JANKOWICZ, *supra* note 14, at 95.

[51] *Id*. at 93.

[52] *Id.* at 95; Sieradzka, *supra* note 45.

[53] JANKOWICZ, *supra* note 14, at 94.

[54] JANKOWICZ, *supra* note 14, at 92; Sieradzka, *supra* note 45.

[55] JANKOWICZ, *supra* note 14, at 94.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

inuring to Russia's benefit and advancing the Kremlin's long-term objectives.[60]

Although the example of Poland's recent experience with its government's use of conspiracy theories as part of a political calculus does not involve a foreign State's cyber-based disinformation,[61] and therefore the questions this Article raises relating to international law are not directly implicated, this example demonstrates some of the potential motivations that a domestic government head may have to remain silent in the face of foreign cyber campaigns using conspiracy theories and disinformation to manipulate democratic opinion-making. These motivations, including domestic political benefits, have been on full display in recent years in the United States.

C. The United States – "Stop the Steal"

Emerging and young democracies like Estonia and Poland may be thought to be more vulnerable to information warfare that seeks to manipulate democratic opinion-making, but established democracies are not immune. If Estonia offers an example of a foreign State's use of disinformation and conspiracy theories to manipulate domestic public opinion in a target State, and if Poland offers an example of information warfare wielded by powerful domestic actors, with an assist from a foreign State, to manipulate public opinion for their own political gain, then the United States offers an example of the two threads woven together.[62] Indeed, one scholar, who has described the tactics used by Russia in the Bronze Night campaign against Estonia as "an early indication" of similarly employed means "that would be unleashed on the United States within a decade"[63] and the use of conspiracy theories by Poland's governing party, PiS, for short-term political gain as "polariz[ing] . . . in the long term,"[64] has observed that the United States government under then-President Donald Trump demonstrated an unsettling willingness to "stealthily crack open the Russian

---

[60] *Id*. at 94-95. Poland is well known for its ability to identify and resist disinformation campaigns originating from Russia, which makes the nation's susceptibility to domestic-based disinformation noteworthy.

[61] Russia does not launch disinformation campaigns to create new messages, but it does make use of "toxic memes" to amplify and to exacerbate societal discord and divisions. LUCAS & POMERANZEV, *supra* note 1, at 30.

[62] *See* discussion *infra* at notes 116-121and accompanying text.

[63] JANKOWICZ, *supra* note 14, at 23.

[64] *Id.* at 203.

playbook for political gain."[65] Following Trump's lead, other domestic actors, including a major political party and its politically sympathetic news media, have now adopted the same active measures against the American public that have previously been the province of malign foreign actors, elevating disinformation and mainstreaming conspiracy theories.[66] For example, Republican lawmakers were quick to adopt a conspiracy theory that Ukraine, not Russia, interfered in the 2016 U.S. presidential election.[67] Despite warnings from national security experts about the danger to U.S. national security interests that these active measures pose,[68] domestic actors have continued—indeed, have redoubled their efforts—to seed one particularly insidious disinformation campaign: that the 2020 presidential election was stolen from the Republican candidate through fraud or other unlawful means.[69] The various elements of this campaign have created

---

[65] *Id.* (providing examples and arguing that "[t]he United States has ventured farther down this road than any other government profiled in [Jankowicz's] book").

[66] *See* Heather Digby Parton, *"Stop the Steal" is Becoming the GOP's Permanent Rallying Cry*, SALON, May 10, 2021 ("Because . . . the entire party from Ted Cruz, R-Tx., and Marjorie Taylor Green, R-Ga, to House Minority Leader Kevin McCarthy, R-Calif., [is] all buying into the notion that Trump's Jan. 6th gambit to overturn the election was legitimate, it's clear that's become conventional wisdom in the GOP as well.").

[67] David Smith, *Fiona Hill: Stop 'Fictional Narrative' of Ukraine Meddling in US Election*, THE GUARDIAN, Nov. 21, 2019 ("Some Republicans on the [House] intelligence committee have pushed a discredited conspiracy theory, embraced by Trump and amplified by conservative media, that Ukraine, rather than Russia, meddled in the last election."); Jake Tapper, *GOP-led Committee Probed Possible Ukraine Interference in 2016 Election and Found Nothing Worth Pursuing, Sources Say*, CNN, Dec. 3, 2019 ("Some Republican lawmakers continue to misleadingly say that the government of Ukraine interfered in the 2016 election on the same level as Russia, despite the GOP-led committee looking into the matter and finding little to support the allegation....The conspiracy theory that Ukraine, not Russia, interfered in the US election was pushed publicly by Russian President Vladimir Putin in February 2017 and has been since pushed by Trump, his attorney Rudy Giuliani, and—most recently—Sen. John Kennedy, a Republican of Louisiana.").

[68] For example, during testimony to the House Intelligence Committee, Fiona Hill, former National Security Council Director for European and Russian Affairs, warned committee members: "Based on questions and statements I have heard, some of you on this committee appear to believe that Russia and its security services did not conduct a campaign against our country – and that perhaps, somehow, for some reason, Ukraine did. This is a fictional narrative that has been perpetrated and propagated by the Russian security services themselves." Smith, *supra* note 67.

[69] Atlantic Council's Digital Forensic Research Lab, *#StopTheSteal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection*, JUST SECURITY

disturbing consequences for the body politic, including, among other things, undermining public trust in the nation's election integrity and other democratic institutions; creating a false perception of illegitimacy of the current administration; and stoking extremist violence against government officials.[70] Together, these efforts undermine the U.S. constitutional and democratic order.[71] And illiberal foreign regimes have noticed. They have used social and traditional media to amplify, and, in some cases, to generate the conspiracy theories and disinformation campaigns, with the goal of dismantling western liberal democracies.[72]

When the government leader of a democratic country which has been targeted by a foreign State with political information warfare intentionally advances the same false narratives, questions necessarily arise concerning the extent, if any, to which the foreign State has successfully corrupted or compromised the target State's leader.[73] Such is the situation in which the United States currently finds itself. Today's Republican Party in the United

---

(Feb. 10, 2021), https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-leading-to-1-6-insurrection/.

[70] *See, e.g.*, Harry Enten, *Polls Show Majority of Republicans Mistakenly Think the 2020 Election Wasn't Legitimate*, CNN (Apr. 11, 2021), https://www.cnn.com/2021/04/11/politics/voting-restrictions-analysis/index.html;
Atlantic Council's Digital Forensic Research Lab, *supra* note 69 (reporting on alleg ed kidnaping plot against Michigan Governor Gretchen Whitmer).

[71] *See, e.g.*, *Warning of a Democracy in Peril, Harvard Scholars Join National Call for Federal Action to Protect Elections*, HARV. KENNEDY SCH. (June 8, 2021), https://www.hks.harvard.edu/faculty-research/policy-topics/democracy-governance/warning-democracy-peril-harvard-scholars-join; Allison Durkee, *Ex-Election Security Chief Krebs Says GOP's Refusal to Concede Election 'Corrosive' To Democracy*, FORBES (Dec. 16, 2020), https://www.forbes.com/sites/alisondurkee/2020/12/16/ex-election-security-chief-chris-krebs-says-gop-refusal-to-concede-election-corrosive-to-democracy/?sh=49b2320d9c01.

[72] JANKOWICZ, *supra* note 14, at xvii:

> Unlike Soviet propaganda, which sought to promote a specific communist-centric worldview, the Kremlin divides and deceives populations around the world, with one goal in mind: the destruction of Western democracy as we know it. Russian deceptions exploit fissures in targeted societies to sow doubt, distrust, discontent and to further divide populations and their governments. The ultimate goal is to undermine democracy—and in particular, the American variety...—and drive citizens to disengage.

[73] Further, to the extent that the government leader's political party follows suit, similar questions abound concerning their support for foreign-sourced disinformation campaigns against the members of their own polity.

States, at the behest of the party leader and former head of state, has all too readily embraced multiple conspiracy theories and disinformation campaigns, and it appears even to have initiated a few of its own.[74] The most pernicious of these efforts, at least as far as the health of American democracy is concerned, is the propagation of the baseless claim that the Democratic Party's candidate for the 2020 presidential election, Joseph R. Biden, III, had "stolen" the election from the Republican Party's candidate, Donald J. Trump, by, among other things, conspiring with voting machine manufacturers to switch votes that had been cast for Trump by recording them as votes cast for Biden.[75] Multiple official recounts, including some hand recounts, have vindicated the conclusion—reached by state election officials, then-Director of the Cybersecurity and Infrastructure Security (CISA) Agency Christopher C. Krebs, and then-Attorney General William P. Barr—that the election results were not tainted, that there was no evidence of significant or widespread voter fraud, and that Biden was the legitimate winner of the presidential election.[76]

Nevertheless, federal and state Republican elected officials, pressed and pressured by Trump and his close allies, continued the disinformation campaign across media platforms of every kind (social media, television, radio, and newspapers), advancing and refining the conspiracy theory that Trump had actually won the election; that Biden's win was illegitimate because of rampant voter fraud and vote tampering; that the results of the election should therefore be overturned; and that Trump should be installed as President for second term.[77] For months, right-wing commentators in legacy media and on social media would continue to repeat the baseless

---

[74] *See* David Atkins, *The Conspiracy Theories A Conservative Must Believe Today*, WASH. MONTHLY (Nov. 10, 2019), https://washingtonmonthly.com/2019/11/10/the-conspiracy-theories-a-republican-must- believe-today/.

[75] *See, e.g.*, Erik Maulbetsch*, Candidates to Lead CO Republican Party Embrace Election Conspiracy Theories*, COLO. TIMES RECORDER (Jan. 28, 2021), https://coloradotimesrecorder.com/2021/01/candidates-to-lead-co-republican-party-embrace-election-conspiracy-theories/34091/.

[76] Michael Balsamo, *Disputing Trump, Barr Says No Widespread Election Fraud*, AP NEWS (Dec. 1, 2020) https://apnews.com/article/barr-no-widespread-election-fraud-b1f1488796c9a98c4b1a9061a6c7f49d; Durkee, *supra* note 71; Tim Reid, *Former Head of U.S. Election Security Calls Trump Team Fraud Allegations "Farcical"*, REUTERS (Nov. 27, 2020), https://www.reuters.com/article/us-usa-election-krebs-idUSKBN28801G; Nick Corasaniti, et al., *The Times Called Officials in Every State, No Evidence of Voter Fraud,* N.Y. TIMES (Nov. 10, 2020) https://www.nytimes.com/2020/11/10/us/politics/voting-fraud.html.

[77] Atlantic Council's Digital Forensic Research Lab, *supra* note 69.

claims by Trump and his enablers in the Republican Party, first that Democrats would steal, then that they had stolen, the election through a massive scheme of voter fraud, vote flipping by electronic voting machines, and other means of cheating throughout closely contested states, such as Georgia, Michigan, Pennsylvania, and Arizona.[78] Despite public assurances from top election officials—in states where Biden had narrowly won—that the elections were safe, secure, and fraud-free and that the vote tallies were accurate, despite similar assurances from Trump's own appointees in the top positions at CISA and the Department of Justice, despite multiple recounts and official audits verifying the election results, despite dozens of failed lawsuits seeking to overturn the election results without credible evidence of fraud or inaccurate vote tallies—despite all of this—Trump, his media allies, and his political supporters in federal and state public office continued to propagate the conspiracy theory (or, more accurately, to an inchoate collection of disparate but occasionally overlapping conspiracy theories) advancing the false assertion that Trump, not Biden, was the legitimate winner of the 2020 presidential election.[79] This assertion, in turn, ignited the "Stop the Steal" social media campaign, hawked extensively by Trump and his political allies, which called for Trump supporters to march on the U.S. Capitol on January 6, 2021, and stop the official counting of the electoral votes as the only way to "save" the country.[80]

The messaging adopted around the 2020 "Stop the Steal" campaign mirrored the narrative adopted by Trump and his political surrogates four years earlier, during the 2016 presidential campaign, when he began declaring in the summer leading up to the election that the only way he would

---

[78] *See, e.g.*, Reality Check Team, *US election 2020: Fact-checking Trump Team's Main Fraud Claims*, BBC NEWS (Nov. 23, 2020), https://www.bbc.com/news/election-us-2020-55016029; Atlantic Council's Digital Forensic Research Lab, *supra* note 69.

[79] Atlantic Council's Digital Forensic Research Lab, *supra* note 69; Madeline Peltz, et al., *On YouTube, The Epoch Times Promoted "Stop the Steal" Events and Spread Misinformation Before and After Capitol Riots*, MEDIA MATTERS (Jan. 26, 2021), https://www.mediamatters.org/epoch-times-and-ntd/youtube-epoch-times-promoted-stop-steal-events-and-spread-misinformation-and; Brian Fung & Donie O'Sullivan, *"Stop the Steal" Groups Hide in Plain Sight on Facebook*, CNN (Jan. 15, 2021), https://www.cnn.com/2021/01/15/tech/facebook-stop-the-steal-evasion/index.html; Nick Robins-Early, *Fox News' Biggest Hosts Go Full Election Conspiracy For Trump*, HUFFPOST (Nov. 6, 2020), https://www.huffpost.com/entry/fox-news-election-trump-hannity_n_5fa5b864c5b64c88d400747f.

[80] Atlantic Council's Digital Forensic Research Lab, *supra* note 69.

lose is if his opponent, Democrat Hillary Rodham Clinton, were to cheat.[81] Amidst constant claims that the 2016 election was "rigged" against Trump, other, more lurid conspiracy theories abounded, as well, some of which were amplified (and perhaps originated with) online Russian operatives.[82] One conspiracy claimed that the murder of a staffer for the Democratic National Convention, Seth Rich, was a professional hit job orchestrated by Clinton.[83] Another, dubbed "Pizzagate", spread spurious allegations of a child sex-trafficking ring headed by Clinton and operated from the basement of a pizza restaurant in Washington, D.C.[84]

---

[81] *Id*. In fact, Trump's close ally and advisor Roger Stone had first employed the phrase even earlier to defend Trump's Republican primary victory. Michael Edison Hayden, *Far Right Resurrects Roger Stone's #StopTheSteal During Vote Count*, SOUTHERN POVERTY L. CTR (Nov. 6, 2020), https://www.splcenter.org/hatewatch/2020/11/06/far-right-resurrects-roger-stones-stopthesteal-during-vote-count.

[82] Salvador Hernandez, *Russian Trolls Spread Baseless Conspiracy Theories Like Pizzagate and QAnon After the Election*, BUZZFEED NEWS (Aug. 15, 2018), https://www.buzzfeednews.com/article/salvadorhernandez/russian-trolls-spread-baseless-conspiracy-theories-like.

[83] Colleen Shalby, *How Seth Rich's Death Became an Internet Conspiracy Theory*, THE LOS ANGELES TIMES (May 24, 2017), https://www.latimes.com/business/hollywood/la-fi-ct-seth-rich-conspiracy-20170523-htmlstory.html ("Two weeks before the Democratic National Convention in July, Democratic National Committee staffer Seth Rich was shot and killed in his Washington neighborhood. His family and Metropolitan D.C. police have said his death was the result of a botched robbery. But conspiracy theories have circulated in right-wing and conservative social and news media spheres fueling unsubstantiated rumors that Rich's killing was political in nature."). For a description of how the conspiracy theory spread, *see* Jeff Guo, *The Bonkers Seth Rich Conspiracy Theory, Explained*, VOX (May 24, 2017), https://www.vox.com/policy-and-politics/2017/5/24/15685560/seth-rich-conspiracy-theory-explained-fox-news-hannity. *See also* Nicole Hemmer, *Sean Hannity Isn't a Leader. He's Just a Fan of Powerful Republicans*, THE WASHINGTON POST (Apr. 20, 2018), https://www.washingtonpost.com/outlook/sean-hannity-isnt-a-leader-hes-just-a-fan-of-powerful-republicans/2018/04/20/7d3397cc-43f9-11e8-8569-26fda6b404c7_story.html (Reporting that for several weeks during 2017, Fox News host Sean Hannity "propagated the strange conspiracy that Hillary Clinton's campaign was somehow responsible for the death of Democratic National Committee staffer Seth Rich, which naturally piqued Trump's interest.").

[84] Joshua Gillin, *How Pizzagate Went from Fake News to a Real Problem for a D.C. Business*, POLITIFACT (Dec. 5, 2016), https://www.politifact.com/article/2016/dec/05/how-pizzagate-went-fake-news-real-problem-dc-busin/ ("Fake news became all too real over the weekend after a North Carolina man entered a Washington pizzeria with an assault rifle in an attempt to 'self-investigate' a false but persistent conspiracy theory about Hillary Clinton. The baseless theory is that the business was a front for a child sex ring run by Hillary Clinton and her campaign manager.").

In both elections, the disinformation campaigns and conspiracy theories propagated by Trump and his domestic allies found inauthentic amplification by foreign-sourced bots and trolls on social media.[85] In addition to creating and boosting conspiracy theories, in 2016, the Russian government, using intelligence agents, proxies, and cutouts, sought to assist Trump's campaign by secretly hacking into the Democratic National Committee's servers, stealing Clinton's emails, and releasing them to the public through WikiLeaks.[86] On several occasions, Trump and his campaign openly used social and traditional media to encourage these efforts. At a press conference in July 2016, five days after WikiLeaks had released the first batch of hacked emails, Trump responded to a reporter's question about possible Russian interference in the election by effectively inviting more of it, when, in reference to missing emails from Clinton's server, he stated: "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing. I think you will probably be rewarded mightily by our press."[87] During the final weeks before the election, between October 10 and November 4, 2016, Trump repeatedly promoted the WikiLeaks dumps at his campaign rallies, proclaiming his "love" for WikiLeaks on more than one occasion.[88] He also used social media platforms to do the same. For example, a few days after WikiLeaks released a tranche of the DNC-hacked emails written by Clinton's Chief of Staff, John Podesta, Trump posted the

---

[85] Hernandez, *supra* note 82 (describing amplification and sourcing of conspiracy theories in the lead-up to the 2016 election); Joseph Menn, *Russian-backed Organizations Amplifying QAnon Conspiracy Theories*, *Researchers Say*, REUTERS (Aug. 24, 2020), https://www.reuters.com/article/us-usa-election-qanon-russia/russian-backed-organizations-amplifying-qanon-conspiracy-theories-researchers-say-idUSKBN25K13T ("Russian government-supported organizations are playing a small but increasing role amplifying conspiracy theories promoted by QAnon, raising concerns of interference in the November [2020] U.S. election.").

[86] Duncan B. Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention?*, OPINIO JURIS (July 25, 2016), http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/ ("U.S. officials and certain cybersecurity experts . . . have concluded Russian government agencies bear responsibility for hacking the Democratic National Committee's servers *and* leaking internal emails stored on them to WikiLeaks…").

[87] *Quoted in* David A. Graham, *Trump's Call for Russian Hacking Makes Even Less Sense After Mueller*, ATLANTIC (Mar. 27, 2019), https://www.theatlantic.com/politics/archive/2019/03/reviewing-trumps-call-russian-hacking-after-mueller/585838/.

[88] David Choi and John Haltiwanger, *5 Times Trump Praised WikiLeaks During His 2016 Election Campaign*, BUS. INSIDER (Apr. 11, 2019), https://www.businessinsider.com/trump-WikiLeaks-campaign-speeches-julian-assange-2017-11.

following message on his Twitter account: "I hope people are looking at the disgraceful behavior of Hillary Clinton as exposed by WikiLeaks. She is unfit to run."[89] In a subsequent Twitter post a day later, he raised the specter of election fraud, stating: "Very little pick-up by the dishonest media of incredible information provided by WikiLeaks. So dishonest! Rigged system!"[90] Trump continued promoting the WikiLeaks releases, using them to elevate the "rigged election" theme throughout the final weeks of the campaign, even though no evidence existed to support his claim, even though cybersecurity experts and the U.S. government had concluded that WikiLeaks was working in concert with Russian intelligence, and even though the CIA had briefed Trump that the emails released by WikiLeaks came from the Russian hack of the DNC server.[91]

The extent to which Trump and his close circle knew that they were adopting and advancing tactics and narratives that were part of a foreign disinformation campaign remains unclear, but their conduct during the 2016 election, in light of public information and reported private briefings from U.S. intelligence connecting Russia to the hacks and leaks, and the lack of candor—indeed, the outright obstruction—by Trump and his campaign aides during the various investigations seeking to understand the Kremlin's role in attacking the integrity of the 2016 U.S. presidential election, raises legitimate

---

[89] *Quoted in* Max Kutner, *Did Trump Know About Democratic Email Theft? Full Timeline of President's WikiLeaks Comments*, NEWSWEEK (Mar. 1, 2018), https://www.newsweek.com/trump-WikiLeaks-comments-timeline-dnc-hacking-mueller-824898.

[90] *Id*.

[91] For an excellent and detailed explanation of Russia's hacking operation and its reliance on WikiLeaks to release the stolen emails, *see* Thomas Rid, *How Russia Pulled Off the Biggest Election Hack in U.S. History*, ESQUIRE (Oct. 20, 2016), https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/. For his part, well after the 2016 election, President Barack H. Obama sought to draw public attention to the malign foreign operations, describing the hacking and release of DNC emails as a breach of "established international norms of behavior." Press Release, *Statement by President on Actions in Response to Russian Malicious Cyber Activity and Harassment*, THE WHITE HOUSE, OFF. PRESS SEC'Y (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [https://perma.cc/T6UC-6K2Z]. A Senate Intelligence Committee Report released in February 2020 noted that President Obama had failed to act more aggressively before the election—while the foreign interference was ongoing—because of his concerns that his response would be perceived as motivated by political considerations rather than concerns about protecting the nation's election security. S. REP. NO. 116-290, vol. 3 at 19 (2020).

concerns.[92] This is especially so given Trump's unwillingness to admit that Russia had interfered on his behalf (despite the intelligence community's high degree of confidence in attributing the interference to Russia), his unexplained personal affinity for Russian President Vladimir Putin, and his continued use of disinformation and conspiracy theories throughout his four years in office in service of his own political fortunes.[93]

---

[92] For example, on August 21, 2016, just a few weeks before WikiLeaks started releasing Podesta's stolen emails, Roger Stone, one of Trump's close advisors, posted the following—at the time, cryptic—statement on Twitter: "Trust me, it will soon be Podesta's time in the barrel." *Quoted in* Emily Shultheis, *John Podesta Suggests Trump Camp Had Warning of WikiLeaks Hack*, CBS NEWS (Oct. 12, 2016), https://www.cbsnews.com/news/john-podesta-suggests-trump-campaign-may-have-had-advanced-warning-of-WikiLeaks-hack/. Although Stone denied that he had any involvement or forewarning about the leaks, a federal criminal indictment, on which Stone was subsequently convicted for witness tampering, making false statements, and obstruction, alleged, in part:

> a. On multiple occasions, STONE told senior Trump Campaign officials about materials possessed by Organization 1 and the timing of future releases.
> b. On or about October 3, 2016, STONE wrote to a supporter involved with the Trump Campaign, "Spoke to my friend in London last night. The payload is still coming."
> c. On or about October 4, 2016, STONE told a high-ranking Trump Campaign official that the head of Organization 1 had a "[s]erious security concern" but would release "a load every week going forward."

Indictment at 17, United States v. Roger Jason Stone, Jr., No. 1:19-cr-00018-ABJ (D.C. Cir. Jan. 24, 2019). In addition, earlier in the campaign, Trump's eldest son, Donald Trump, Jr., had expressed an enthusiastic willingness to meet with a person described to him as a Russian government official who had incriminating evidence about Clinton to share with him and that the information was "part of Russia and its government's support for Mr. Trump," by replying, "If it's what you say I love it especially later in the summer." *Quoted in* Andrew Rafferty, *Trump Jr. Emails: 'I Love It' When Offered Russian Info on Clinton*, NBC NEWS (July 11, 2017), https://www.nbcnews.com/politics/politics-news/trump-jr-tweets-his-emails-led-russia-meeting-n781736.

[93] Graham, *supra* note 87. These concerns are particularly salient for purposes of this Article because of the questions they raise regarding international law development in light of Trump's liberal use of the presidential pardon power to pardon, among others tied to Russia's election meddling, Roger Stone and Paul Manafort, both of whom had refused to cooperate with federal prosecutors investigating Trump's role in Russia's interference in the 2016 election. *See* Doha Madani, *Trump Pardons Roger Stone, Paul Manafort, Charles Kushner and Others*, NBC NEWS (Dec. 23, 2020), https://www.nbcnews.com/politics/politics-news/trump-pardons-roger-stone-paul-manafort-charles-kushner-others-n1252307.

Four years later, by the time the 2020 presidential election results were counted, the willingness of Trump and his political allies to spread Russian disinformation could not be attributed to ignorance about its purpose or provenance. The farther into Trump's tenure in office, the more difficult it became to distinguish the disinformation campaigns that originated with foreign governments and were advanced by domestic political actors from the disinformation campaigns that originated with domestic political actors and were advanced by foreign governments. At some point, it seems the goals of both seemed to align.[94] The still-thriving "QAnon" conspiracy offers a compelling illustration.[95] According to the Soufan Center, an independent, non-profit organization studying global security, QAnon is a "far-right conspiratorial movement that creates and co-opts 'theories' to fit an evolving narrative underpinned by the core notion that the 'Deep State', led by a cabal

---

[94] Increasingly, historians, political scientists, national security experts, and other experts on authoritarian regimes are sounding the alarm that Trump and the Republican Party are willing to dismantle U.S. democracy to secure and remain in power, which parallels the ultimate goal of the Kremlin. *See, e.g.*, Lois Beckett, *Scholars Warn of Collapse of Democracy as Trump v Biden Election Looms,* GUARDIAN (Nov. 1, 2020), https://www.theguardian.com/world/2020/nov/01/democracy-fascism-global-trump-biden-election; Nancy LeTourneau, *Authoritarianism and the Identity Politics of the Republican Party*, WASH. MONTHLY (Apr. 9, 2018), https://washingtonmonthly.com/2018/04/09/authoritarianism-and-the-identity-politics-of-the-republican-party/; Ivana Kottasova, *US Republicans Are Starting to Look a Lot Like Authoritarian Parties in Hungary and Turkey, Study Finds*, CNN (Oct. 26, 2020), https://www.cnn.com/2020/10/26/world/republican-party-more-illiberal-study-intl/index.html; Christopher Ingraham, *GOP Leaders' Embrace of Trump's Refusal to Concede Fits Pattern of Rising Authoritarianism, Data Shows*, WASH. POST (Nov. 12, 2020), https://www.washingtonpost.com/business/2020/11/12/republican-party-trump-authoritarian-data/; John Haltiwanger, *Republicans Are Putting America's Democracy in Mortal Danger, More than 100 Scholars Warn,* BUS. INSIDER (June 1, 2021), https://www.businessinsider.com/us-democracy-danger-gop-voting-restrictions-over-100-scholars-warn-2021-6; HARV. KENNEDY SCH., *supra* note 71.

[95] *See* AP, *Lies, Disinformation and Conspiracy Theories are Increasingly Being Embraced as Acceptable Political Strategy*, AP INVESTIGATION FINDS (Feb. 26, 2021), https://www.marketwatch.com/story/lies-disinformation-and-conspiracy-theories-are-increasingly-being-embraced-as-acceptable-political-strategy-ap-investigation-finds-01614394986; Zachary Cohen, *China and Russia "Weaponized" QAnon Conspiracy Around Time of US Capitol Attack, Report Says*, CNN (Apr. 19, 2021), https://www.cnn.com/2021/04/19/politics/qanon-russia-china-amplification/index.html (describing QAnon as "a sprawling far-right conspiracy theory that promotes the absurd and false claim that former President Donald Trump has been locked in a battle against a shadowy cabal of Satan-worshipping pedophiles made up of prominent Democratic politicians and liberal celebrities.").

of elitist pedophiles, is leading the United States."[96] As Trump and his political supporters and allies have promoted QAnon narratives for the "Stop the Steal" campaign, so, too, have foreign adversaries, such as Russia and China, incorporated QAnon-narratives into their disinformation campaigns aimed at "susceptible audiences in the United States and beyond."[97]

Furthermore, with few exceptions, the entire political party that had supported Trump throughout his tenure in office has joined him in propagating disinformation and conspiracy theory campaigns.[98] Moreover, like Trump, the party has embraced the lie that Biden's electoral victory resulted from massive voter fraud, and they propagated that lie for weeks, and then months, eventually refusing to recognize Biden as the legitimate winner, and, in many instances, echoing Trump's calls to protect the integrity of the nation's elections and to "Stop the Steal."[99] Relying directly or indirectly on "stolen election" conspiracy theories, 126 Republican lawmakers signed an amicus brief,[100] and seventeen Republican Attorneys General signed a separate amicus brief,[101] supporting a lawsuit brought by Texas Attorney General Ken Paxton asking the United States Supreme Court to overturn the results of the 2020 presidential race in Pennsylvania, Georgia, Michigan, and Wisconsin.[102] Worse, on the basis of the false fraud allegations

---

[96] The Soufan Center, *Special Report: Quantifying the Q Conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon* 1*,* 8 (2021), https://thesoufancenter.org/wp-content/uploads/2021/04/TSC-White-Paper_QAnon_16April2021-final-1.pdf.

[97] *Id.*; *See* AP, *supra* note 95; Cohen, *supra* note 95.

[98] *See* Atkins, *supra* note 74.

[99] *See, e.g.*, Sam Levine, *How Republicans Came to Embrace the Big Lie of a Stolen Election*, THE GUARDIAN (June 13, 2021), https://www.theguardian.com/us-news/2021/jun/13/republicans-big-lie-us-election-trump; Chris Cillizza, *88% of House and Senate Republicans Refuse to Publicly Acknowledge the Obvious: Joe Biden Won*, CNN (Dec. 7, 2020), https://www.cnn.com/2020/12/07/politics/donald-trump-joe-biden-2020-election/index.html.

[100] Mot. for Leave to File Br. Amicus Curiae and Br. Of Amicus Curiae U.S. Representative Mike Johnson and 125 Other Members of the U.S. House of Representatives in Supp. Of Pl.['s] Mot. For Leave to File a Bill of Compl. And Mot. For a Prelim. Inj., Texas v. Pennsylvania, et al., 592 U.S. __ (2020) (No. 155).

[101] Br. of State of Mo. and 16 Other States as Amici Curiae in Support of Pl.'s Mot. for Leave to File Bill of Compl., Texas v. Pennsylvania, et al., No. 220551 (2020).

[102] Mot. for Leave to File Bill of Compl., Texas v. Pennsylvania, et al., Doc. 220551, 592 U.S. ___ (2020). The Supreme Court denied the case for lack of standing. Order in Pending Case, Texas v. Pennsylvania, et al., No. 155, Orig., Dec. 11, 2020, https://www.supremecourt.gov/orders/courtorders/121120zr_p860.pdf.

perpetuated by Trump and his acolytes, dozens of Republican lawmakers in both Houses of Congress voted against certifying the election results in key states, despite the absence of any evidence that the election had been fraudulently or otherwise illegitimately tipped in Biden's favor, giving further unjustified credence to the claims of their Party leader, who at the time still occupied the Oval Office and wielded significant levers of government power, that the election had been stolen from him.[103]

During the weeks after the election, a growing chorus of "Stop the Steal" rallying cries gained traction among Trump supporters and amplification from Trump himself.[104] Trump's election campaign funded and organized a "Stop the Steal" rally to take place on the Capitol ellipse on January 6, 2021, the same day that Congress was scheduled to perform what has traditionally been the ministerial task of voting to approve each State's slate of electors, certifying the final election outcome.[105] During a speech at the rally, Trump called on his supporters to go to the Capitol to protest the congressional vote.[106] Following Trump's cue, the rally-goers descended on the Capitol.[107] What had begun as a peaceful rally based on a conspiracy theory and disinformation escalated over the course of the afternoon into a violent insurrection based on a conspiracy theory and disinformation.[108] Though the congressional vote resumed in the hours after the insurrectionists had been subdued and dispersed, the violence that had interrupted the proceedings resulted in multiple deaths and injuries; and though the attack on the Capitol and those inside it was ultimately quelled, the conspiracy

---

[103] Alvin Chang, *The Long List of Republicans Who Voted to Reject Election Results*, GUARDIAN (Jan. 7, 2021), https://www.theguardian.com/us-news/2021/jan/07/list-republicans-voted-to-reject-election-results;
John Bowden, *The Republicans Who Voted to Challenge Election Results*, HILL (Jan. 7, 2021), https://thehill.com/homenews/house/533076-read-the-republicans-who-voted-to-challenge-election-results.

[104] Atlantic Council's Digital Forensic Research Lab, *supra* note 69.

[105] *Id*.

[106] *Id*.

[107] *Id*.

[108] *Id*. Moreover, Republican lawmakers have embraced a host of new conspiracy theories in the aftermath of the January 6 coup attempt, seeking to lay blame for the violence at the Capitol on, in turns, Antifa, Black Lives Matter, and even the Federal Bureau of Investigation. Alex Woodward, *Republicans Blame FBI for Capitol Riot in New Conspiracy*, INDEPENDENT (June 16, 2021), https://www.independent.co.uk/news/world/americas/us-politics/tucker-carlson-capitol-riot-conspiracy-b1867375.html.

theory that produced it has continued to gain momentum.[109] As of this writing, Trump has continued to peddle the falsehood that he was the legitimate winner of the 2020 presidential election;[110] congressional Republicans—with only a handful of exceptions—have either embraced the conspiracy theory that the election was stolen from Trump or have refused to debunk it.[111] In addition, State-level elected Republicans have authorized unofficial "audits" of the vote tallies conducted by a private partisan company with no auditing experience.[112]

---

[109] Tara Subramaniam, *Fact-checking Sidney Powell's Claim Trump Could be Reinstated*, CNN (June 1, 2021), https://www.cnn.com/2021/06/01/politics/powell-trump-inauguration-fact-check/index.html.

[110] D.L. Davis, *Déjà Vu All Over Again as Former President Trump Wrongly Claims Wisconsin Victory*, POLITIFACT (July 6, 2021), https://www.politifact.com/factchecks/2021/jul/06/donald-trump/deja-vu-all-over-again-former-president-trump-wron/; Matt Shuham, *Trump Clings To Big Lie, Claims People Who Didn't Vote Stole Georgia Election*, TALKING POINTS MEMO (June 23, 2021), https://talkingpointsmemo.com/news/trump-clings-to-big-lie-claims-people-who-didnt-vote-stole-georgia-election ("Former President Donald Trump continues to cling to the lie that he won a second term in office, this time on the basis of several thousand soon-to-be purged Georgians who didn't vote in the 2020 presidential election.").

[111] Philip Bump, *A Surreal, Submerged, Conspiratorial, Trump-Centered Political Universe Still Thrives*, WASH. POST (June 1, 2021), https://www.washingtonpost.com/politics/2021/06/01/surreal-submerged-conspiratorial-trump-centered-political-universe-still-thrives/ (observing that political rallies held by some congressional Republicans advance "the same falsehood that Trump has worked to promote since his ouster: that he didn't lose [the presidential election] last year."); David Weigel, *"Trump Won": The Many Ways the GOP is Re-writing 2020*, WASH. POST (June 8, 2021), https://www.washingtonpost.com/politics/2021/06/08/trailer-trump-won-many-ways-gop-is-re-writing-2020/ ("As the year's final state primaries wrap up and the midterm campaign gets underway, Republicans have embraced doubts about the 2020 election, and become more adamant about support for the former president."); Arden Farhi, et al., *We Asked All 50 GOP Senators Whether They Agree with Trump that He Won the Election. Only 5 Responded,* CBS NEWS (Feb. 19, 2021), https://www.cbsnews.com/news/trump-election-republican-senators-5-respond/ (concluding that "the fact that [Senate Republicans] are not speaking out even as Mr. Trump continues to claim he won the election – which the majority of the Senate believes led to the armed insurrection — is a sign of the former president's enduring political clout.").

[112] Mia Jankowicz, *Arizona GOP Official Blasts Company Carrying Out Election Recount: "Insane Just From a Competence Standpoint"*, BUS. INSIDER (June 22, 2021), https://www.businessinsider.com/gop-official-blasts-insane-cyber-ninjas-arizona-audit-as-incompetent-2021-6; Amanda Carpenter, *How the Arizona Cyber Ninjas Audit Happened—In One Easy Step!*, BULWARK (June 28, 2021), https://thebulwark.com/how-the-arizona-cyber-ninjas-audit-happened-in-one-easy-step/.

The consequences of this groundless claim have proven dire for American democracy. According to an April 2021 Reuters/Ipsos poll, more than half of Republican voters wrongly believe that the election was stolen from Trump and that voter fraud or election rigging resulted in Biden's win.[113] As of June 2021, nearly half of Republican voters believe that State legislatures should have the power to declare the winner of an election, even if doing so would overturn the election results that are based on the popular vote count.[114] None of this bodes well for the long-term health and survival of the American republic, but it does cheer America's anti-democratic adversaries. The use of cyber-operations to generate or boost conspiracy theories and disinformation campaigns for the purpose of influencing democratic popular opinion-making has proven an effective tool in the hands of malign foreign governments,[115] especially in situations where a domestic government leader is willing to invite or accept them (and possibly later to adopt similar tactics against the domestic population). As illustrated by the "Stop the Steal" campaign, such activities pose a number of questions about how they should be treated under international law, and the willingness of a domestic head of State to amplify foreign-sourced conspiracy theories and disinformation only creates additional complications.

The genesis of the "Stop the Steal" conspiracy theory and related disinformation remains unclear. Although, at present, no evidence directly implicates the Russian government, Trump advisor Roger Stone began peddling the stolen election narrative in the run-up to the 2016 presidential election, and Trump quickly adopted it, falsely claiming that the only way his opponent could win was if the election were rigged.[116] What is

---

[113] Enten, *supra* note 70 (reporting poll results finding that "55% of Republicans falsely believe Joe Biden's victory in the 2020 presidential election was the result of illegal voting or rigging [and] 60% of Republicans incorrectly agree that the election was stolen from Republican Donald Trump.").

[114] Lee Drutman, *Theft Perception Examining the Views of Americans Who Believe the 2020 Election was Stolen*, DEMOCRACY FUND VOTER STUDY GROUP (June 2021), https://www.voterstudygroup.org/publication/theft-perception.

[115] *See* discussion *supra* Part II.A. For another potent example, see JANKOWICZ, *supra* note 14, at 123-535 (describing successful Russian cyber-based disinformation campaign to persuade Dutch voters to vote no in a referendum on admitting Ukraine to the European Union).

[116] Hayden, *supra* note 81. Also noteworthy is the early adoption of the 2020 "Stop the Steal" campaign and its propagation on social media by Jack Posobiec, a "far-right" commentator on social media, who also works as a correspondent for One America News Network ("OANN"), *see* Atlantic Council's Digital Forensic

noteworthy about Roger Stone's early promulgation of this particular conspiracy theory in 2016 is the similar role he played in promoting the emails that Russia exfiltrated from the Democratic National Convention's servers and subsequently released through WikiLeaks in 2020.[117] Because of that role and his contacts with "Guccifer 2.0" (the persona claiming responsibility for the DNC hack), the Department of Justice Special Counsel, which was appointed to determine whether Trump or individuals associated with his 2016 presidential campaign had coordinated with Russian government officials or cutouts to facilitate Russia's interference with the 2016 election, investigated Stone's contacts and communications, and determined that Stone had lied to Congress about his contacts and had failed to turn over relevant documents.[118] Stone was subsequently indicted and convicted for obstructing a congressional investigation, making false statements to Congress, and tampering with a witness.[119] Trump subsequently pardoned Stone.[120] The through-line of Roger Stone acting as both a close advisor to Trump and as a "Stop the Steal" propagator in both the 2016 and 2020 elections, Stone's contacts with Guccifer 2.0, and his willingness to mislead Congress in its Russia election interference investigation reasonably raise questions about whether Trump himself knowingly promoted a Russian-sourced disinformation campaign.

The through-line of Roger Stone's role in both election campaigns also underscores some of the ambiguities existing under international law with respect to a foreign government's use of information warfare in the form

---

Research Lab, *supra* note 69, which also employs a known Russian-state reporter and is known to advance the Kremlin's disinformation and other propaganda, *see* Kevin Poulsen, *Trump's New Favorite Channel Employs Kremlin-Paid Journalist*, THE DAILY BEAST (July 22, 2019), https://www.thedailybeast.com/oan-trumps-new-favorite-channel-employs-kremlin-paid-journalist?ref=scroll (commenting that OANN has become "increasingly dedicated to conspiracy theories and fake news, and became overtly supportive of Russia's global agenda"); *see also* Kevin Poulsen, *Trump's New Favorite Network Embraces Russian Propaganda*, THE DAILY BEAST (May 3, 2019), https://www.thedailybeast.com/trumps-new-favorite-network-oann-embraces-russian-propaganda.

[117] Atlantic Council's Digital Forensic Research Lab, *supra* note 69.

[118] Robert S. Mueller III, Opinion, *Roger Stone Remains a Convicted Felon, and Rightly So*, WASH. POST (July 11, 2020), https://www.washingtonpost.com/opinions/2020/07/11/mueller-stone-oped/?arc404=true.

[119] Indictment at 17, United States v. Roger Jason Stone, Jr., No. 1:19-cr-00018-ABJ (D.C.Cir. Jan. 24, 2019); Ali Dukakis & Lucien Bruggeman, *Roger Stone Found Guilty on All 7 Counts*, ABC (Nov. 15, 2019), https://abcnews.go.com/Politics/roger-stone-found-guilty-counts/story?id=67015102.

[120] Madani, *supra* note 93.

of conspiracy theories and disinformation campaigns to influence democratic opinion-making by the polity of another State when the target country's head of State remains silent in the face of such information warfare or even actively amplifies it in concert with the hostile foreign government.[121] These ambiguities would likely be exacerbated if the silence of, or amplification by, the target state's head of government were corruptly or complicitly obtained by the hostile State. For example, assuming arguendo, that the "Stop the Steal" campaign is of Russian origin and that Trump knew that fact when he perpetuated it, both in 2016 and in 2020, then the following questions implicating international law arise: first, whether Trump, after assuming office in January 2017, effectively ratified Russia's interference with U.S. democratic opinion-making in the 2016 election because he had previously welcomed the conduct and refused to disavow it later; and second, whether Trump in 2020 effectively (if not actually) consented to Russian cyber operations on his behalf to promote the "Stop the Steal" campaign.

The point here is not to determine whether "Stop the Steal" in either its 2016 or (perhaps especially) its 2020 incarnation was, in fact, a tactic in Russia's ongoing information warfare against the United States and other western democracies, or whether Trump and his associates have knowingly amplified or invited Russian disinformation into the United States electoral discourse. Rather the purpose of the foregoing discussion is to lay the groundwork for exploring the implications for the development of customary international law in situations involving a target State's failure to respond to a hostile State's cyber intrusion into the target State's democratic opinion-making processes because the target State's head of government has corruptly or complicitly consented to the intrusion.

III. THE PERTINENT INTERNATIONAL LAW FRAMEWORK

The use of cyber operations as a means of conducting information warfare is a relatively recent phenomenon, creating the need for governments, practitioners, scholars, and other international law experts to navigate a range of novel issues in international law and its application. The foregoing discussion suggests a number of discrete legal issues that may arise under international law. Among them are which international law norms and principles should apply to cyber activities broadly; which international law norms and principles, if any, should apply to cyber activities at the more specific level of information warfare designed to manipulate the voting

[121] See *infra,* Parts III and IV.

behavior of another State's population (e.g., using cyberspace to promote conspiracy theories and disinformation campaigns); and how, if at all, the international law framework, as applied to cyber-based information warfare, should account for the role that corruption or *kompromat* may play in enabling a perpetrating State to secure the cooperation of a target State's government head (or other organ of the government) in creating or amplifying the foreign State's information warfare. This Part reviews applicable international law principles relating to these questions, including both the background and the current status of those principles as applied to cyber-based activities generally and to online operations targeting voter opinion-making and political preferences. Though the basics are now mostly agreed upon, many core issues remain unsettled, and some peripheral issues have yet to appear on the horizon.

As a preliminary matter, the application of international law to states' cyber-based activities is widely accepted.[122] Specifically, the international community appears to have reached consensus that the international law principles of sovereignty and non-interference apply to states' cyber activities.[123] As early as 2013, the United Nations Group of Government

---

[122] HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION, 4 (Dec. 2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks ("States have agreed that international law, including the principles of sovereignty and non-intervention, does apply to states' activities in cyberspace.").

[123] *Id.* at 8. The international legal framework offers a number of possible approaches for dealing with activities conducted in cyberspace, including information warfare, more generally. One option would be to treat cyber activities that utilize information warfare in the same way that it treats peacetime espionage, which treatment largely leaves any imposed penalties to the domestic law of the targeted State. Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate, International Law?*, 95 TEX. L. REV. 1579, 1582-83 (2017) (noting the consensus opinion that espionage violates domestic law, not international law). Although several rules of international law would seem to forbid espionage, the practice is so widely employed that a consensus among scholars has emerged that customary international law has created a new norm permitting it. MOYNIHAN, *supra* note 122, at 45 (observing that "in the non-cyber context, the majority position among commentators is that with the exception of certain rules, espionage is largely left unregulated by international law and as such is not prohibited by international law per se"). Some scholars reject the conclusion that customary international law has coalesced around a permissive structure for peacetime espionage. *See* Inaki Navarrete and Russell Buchan, *Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions*, 51 CORNELL INT'L L.J. 897, 912-14 (2019) (arguing, contrary to prevailing opinion, that such a norm

Experts (UNGGE) reported agreement among states that, pursuant to the principles of the United Nations Charter, states must observe the principle of sovereignty regarding jurisdiction over infrastructure for information and communications technology that is located within a State's territory and regarding states' cyber-related activities.[124] The 2013 UNGGE report likewise concluded that international norms and principles flowing from sovereignty also apply to states' cyber-related activities.[125] One such principle deriving from sovereignty is the principle of non-intervention.[126] Beyond this baseline agreement, however, the particulars of how international law applies to cyber activities are unresolved, resulting in ambiguities relating to states' legal rights and obligations in the cyber

---

does not, in fact, exist because much of the conduct characterized as peacetime espionage is conducted surreptitiously and therefore cannot meet the State practice requirement for establishing customary international law). Under this approach, cyber operations, like espionage, would be subject to sanction only if they violated some domestic law of the target rather than being treated as "internationally unlawful per se." MOYNIHAN, *supra* note 122. If this approach were taken, however, it would require justification for enveloping cyber operations into definitions and conceptions of espionage currently in place in international law; otherwise, this approach would require a wait-and-see posture to allow customary international law to develop (or not) cyber norms similar to those governing non-cyber espionage. *See Id*. at 46-47 (arguing that cyber espionage activities should be evaluated individually to determine whether they violate other binding norms under international law). A second option would be to develop new international rules and principles designed specifically for cyberspace, including the use of cyberspace for conducting information warfare. *Id*. at 7. Based upon the premise that cyber activities present unique circumstances and challenges, this approach presumes that the existing principles and norms governing international law cannot properly address the ranges of issues at play in the cyber context. At present, however, international law experts have opted for a third approach, reaching the general consensus that the current international law framework can adequately accommodate emerging cyber-related issues, including information warfare conducted in cyberspace, without creating new, cyber-specific rules or treating them as functionally equivalent to peacetime espionage. Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1639 n. 3 (2017) ("There appears to be near-universal consensus that the extant international law governs cyber activities."). This approach could still ultimately allow for treating cyber activities in the same way as espionage, but the trend is not currently flowing in that direction.

[124] Rep. of the Group of Governmental Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Security, ¶ 19, U.N. Doc. A/68/98 (2013).

[125] *Id.* ¶ 20. These conclusions were also reiterated in the UNGGE 2015 Report. Rep. of the Group of Governmental Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Security, ¶¶ 27-28, U.N. Doc. A/70/174 (2015).

[126] Rep. of the Group of Governmental Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Security, ¶ 28b, U.N. Doc. A/70/174 (2015).

context.[127] More specifically, the ways in which those principles are to be applied to specific categories of State cyber conduct lack clarity, as does the underlying predicate for what constitutes a violation justifying a right of response.[128] These issues become especially thorny when determining how international law applies to the particular type of cyber activity under scrutiny in this Article, namely a State's cyber-based operations that propagate and amplify conspiracy theories and disinformation campaigns targeting democratic opinion-making in another State. They become even thornier if the government leader of the target State remains silent and passive in the face of such operations, and they become thornier still if the target State's silence and passivity have been corruptly obtained by the infringing State. This Part provides a brief overview of the applicable international law principles and the issues raised by their application to cyber-based operations, including information warfare designed to affect the voting behavior of another State's populace, before the following two Parts discuss, in turn, the difficulties that states' silence pose for the development of customary international law in this area, and the additional analytical problems that may warrant consideration in instances where domestic corruption motivates a State's response to these kinds of foreign cyber activities.

A. Applicable Principles: Sovereignty and Non-intervention

Within the widely accepted view that international law principles, including the principles of sovereignty and non-intervention, apply to cyber activities broadly understood, uncertainty nonetheless exists, about which principle or principles should apply to particular cyber activities. Some of that uncertainty results from differences in conceptions about the principles themselves. Some of it results from the nontraditional features of the cyber activities. And some of it results from the still-developing nature of State practice in response to hostile cyber operations conducted remotely. This section considers the interplay between these sources of uncertainty.

---

[127] MOYNIHAN, *supra* note 122, at 4. This is so in part because states have been reluctant to make public their views on how international law precepts apply to cyber operations, and cyber operations themselves are usually conducted surreptitiously, making the drawing of reliable inferences difficult. *Id*. at 6; Barela, *supra* note 8 ("[W]hen it comes to cyberspace there are a host of difficulties for articulating the precise application of international law. Agreement among States has been slow due to the many new challenges posed by rapidly expanding networks of information and communication technologies (ICTs).").

[128] MOYNIHAN, *supra* note 122, at 4.

1. Sovereignty

Sovereignty is a principle of international law giving rise both to rights that a State enjoys in relation to other states and to duties that a State must fulfill in relation to other states.[129] Under this principle, a State possesses "the supreme authority . . . to territorial integrity, sovereign equality and political independence within its territory to the exclusion of all other states."[130] Major cases decided by international tribunals affirm these aspects of sovereignty. For example, in the *Corfu Channel* case, in which the International Court of Justice (ICJ) concluded, *inter alia*, that the United Kingdom had violated the sovereignty of the Republic of Albania by conducting minesweeping operations in Albanian territorial waters without the consent of the Albanian government, the majority opinion stated: "Between independent states, respect for territorial sovereignty is an essential foundation of international relations."[131] In a concurring opinion, Judge Alvarez explained further: "By [sovereignty], we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other states, and also in its relations with other states."[132]

A different tribunal, the Permanent Court of Arbitration, deciding a case in which the United States and the Netherlands laid conflicting claims to the Island of Palmas (or Miangas), observed: "[T]erritorial sovereignty belongs always to one, or in exceptional circumstances to several states, to the exclusion of all others."[133] The right to exclude others is related to, but distinct from, the sovereign right of political independence, which recognizes a State's sole authority to exercise "the functions of a State" within its territory.[134] Stated differently, "[t]erritorial sovereignty . . . involves the exclusive right to display the activities of a State."[135]

---

[129] Memorial of United Kingdom, Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 43 (April 9) (separate opinion by Alvarez, J.) ("Sovereignty confers rights upon States and imposes obligations on them.").

[130] MOYNIHAN, *supra* note 122 at 8.

[131] Memorial of United Kingdom, Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 35 (April 9) (separate opinion by Alvarez, J.).

[132] *Id*. at 43.

[133] Island of Palmas (U.S. v. Neth.), Hague Ct. Rep. 2d (Scott) 838 (Perm. Ct. Arb. 1928).

[134] *Id*.

[135] *Id*. at 839.

When a State engages in cyber activities that do not involve the use of force,[136] the standard against which to measure whether such activities violate international law—thereby triggering a right of response—is unclear, but two broad approaches have emerged in the relevant legal commentary.[137] Some commentators have taken the position that a State's cyber activity below the use of force violates international law and gives rise to a right of response only if the intrusion runs afoul of the non-intervention principle.[138] Those adhering to this philosophy view sovereignty in the cyber context as a guiding principle that may inform states in their conduct relating to cyberspace rather than as "a standalone rule" which itself may be violated. In other words, if the requirements for a violation of the non-intervention principle—including the requirement of coercion—are not met, then the cyber activity in question does not violate international law.[139] Other commentators have taken the position that a State's cyber intrusions need not meet the non-intervention threshold to constitute an unlawful violation of the target State's sovereignty. On this view, sovereignty is a standalone primary rule, the breach of which authorizes response by the target State under international law.[140]

State practice regarding these two approaches remains in a state of flux.[141] The United States, for example, at one time appeared to adopt (or at

---

[136] Article 2 of the United Nations Charter "prohibits the threat or use of force and calls on all Members to respect the sovereignty, territorial integrity and political independence of other States." U.N. Charter art. 2, ¶ 4.

[137] Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: An Analysis*, JUST SECURITY (Oct. 14, 2019), https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ (describing disagreement among international law experts and divergence in State practice on the question of whether sovereignty is itself "a *rule* of law that . . . may be violated.").

[138] *See* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace,* 42 YALE J. INT'L L. ONLINE 1, 4-5 (2017) (explaining competing approaches to the sovereignty principle).

[139] See *infra,* Part II.A.2 for discussion of the coercion element.

[140] *See, e.g*., Schmitt & Vihul, *supra* note 123 (arguing that "overwhelming evidence of State practice and *opinio juris*–the foundational elements of customary international law–supports the assertion" that sovereignty operates as a primary rule rather than a guiding principle.).

[141] MOYNIHAN, *supra* note 122, at 8-9 (explaining that states have opted for a "'policy of ambiguity and silence'" on this question. *Id*. at 9, quoting another source). Moreover, no treaties are in place to fill the gap left by the decision of most states not to "put on the record how they think these principles apply in practice." *Id*. at 10

least to be open to adopting) the "sovereignty as rule" approach when the Department of Defense opined in 1999 that at least some cyber activities undertaken by a State against another State could violate the target State's sovereignty, thereby constituting an "internationally wrongful act."[142] More recently, the United States appears to have drifted toward the school of thought that conceives of sovereignty in the cyber context as an underlying principle to guide the establishment of binding norms rather than a rule of international law that itself can be breached and thereby result in an international obligation.[143] Although the United Kingdom also tacks in the same direction,[144] the sovereignty-as-principle-only position runs counter to the consensus of the international group of experts reported by the Tallinn Manual 2.0, which adopted the "sovereignty-as-rule" approach to cyber operations.[145]

The difference between these two approaches to sovereignty, that is, between sovereignty-as-principle-only and sovereignty-as-rule, has implications for how international law is to treat a foreign State's cyber operations that involve propagating conspiracy theories and disinformation campaigns in a target State in an attempt to manipulate the target State's democratic decision-making. If sovereignty is a primary rule of international law, then a remote cyber operation may violate sovereignty if the operation either manifests on the territory of the target State or if it "interferes with or usurps inherent governmental functions of [the target] state."[146] An example of a territorial manifestation of a remotely conducted cyber operation

---

(noting the exception of the Council of Europe's Budapest Convention, which covers cybercrimes).

[142] Schmitt & Vihul, *supra* note 123, at 1640.

[143] Schmitt & Vihul, *supra* note 123, at 1640-42.

[144] MOYNIHAN, *supra* note 122, at 8 and n. 28.

[145] Schmitt & Vihul, *supra* note 123, at 1640-42 ("Tallinn Manual 2.0 accordingly provides in Rule 4 that '[a] State must not conduct cyber operations that violate the sovereignty of another State.'") *Id*. at 1642; *see also* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace,* 42 YALE J. INT'L L. ONLINE 1, 5 (2017) ("This 'sovereignty as principal, but not rule' approach contradicts extensive State practice and *opinio juris* in the non-cyber context, which treat the *prohibition* as a primary rule, such that a violation of sovereignty would constitute an internationally wrongful act.").

[146] Schmitt, *supra* note 137; Schmitt & Vihul, *supra* note 123, at 1649 (arguing that cyber operations which interfere with or usurp a State's inherently governmental functions constitute a violation of sovereignty, regardless of whether such operations cause damage or injury within the target State, and regardless of the infringing State's use of coercion). Elections are considered an inherently governmental function. MOYNIHAN, *supra* note 122, at 40.

constituting a violation of sovereignty is physical damage to the target State's infrastructure.[147] An example of an inherent government function—that is, a function that only states may undertake (or authorize other entities to undertake)—is conducting elections.[148] If sovereignty is only a guiding principle, the violation of international law for conducting remote cyber operations must be based upon some other principle that does constitute a binding rule, such as the non-intervention principle.

2. Non-intervention

The non-intervention principle prohibits a State from intervening in another State's internal affairs, even when such intervention does not involve the use of force.[149] More precisely, it prohibits coercive conduct by one State "in relation to the inherently sovereign powers of another state."[150] Like the principle of sovereignty, the non-intervention principle has been affirmed in multiple decisions by international tribunals. In 1986, the ICJ, for example, observed in the *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)* that "[t]he principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference, [and] the Court considers that it is part and parcel of customary international law."[151] Elaborating, the Court continues:

> A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[152]

---

[147] Schmitt, *supra* note 137.

[148] *Id*.

[149] Hollis, *supra* note 86 ("[c]ustomary international law has long recognized a 'duty of nonintervention' that applies to State behavior . . . falling short of the use of force."); Schmitt, *supra* note 137 (observing that non-intervention prohibits a foreign State from using coercion to affect an activity that falls within the target State's "domaine réservé," including, for example, elections.).

[150] MOYNIHAN, *supra* note 122, at 8.

[151] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J. 14, ¶ 202 (June 27).

[152] *Id.* ¶ 205.

Despite "widespread consensus that a duty of non-intervention *is* customary international law," however, "the scope and substance of the duty remain unclear."[153] This lack of clarity exists partly because coercion, while an essential element of a violation of the non-intervention principle, does not enjoy an accepted international law definition.[154] Although the use of force clearly constitutes coercive intervention, measures that do not reach the level of force generate disagreement about where, and how, to draw the line between the permissible, i.e., that conduct which falls on the "noncoercive" side of the divide, and the impermissible, i.e., that conduct which falls on the "coercive" side of the divide.[155] Of course, how coercion is defined will determine not only whether any given cyber operations violate the non-intervention principle, but also, by extension, whether the target State enjoys a right of response under international law.[156]

Consider the following examples: One definition of coercion is "compelling a state to take a course of action (whether an act or omission) that it would not otherwise pursue."[157] Under this definition, the use of cyber operations to influence the target State is distinguished from the use of cyber operations to coerce the target State.[158] The former, an example of which is "a powerful social media campaign designed to affect elections", does not meet the standard established by the above definition of coercion and does not, therefore, violate the non-intervention prohibition.[159] The latter, an example of which is the manipulation of election results, does meet the standard for coercion under the above definition, and does, therefore, qualify as impermissible intervention.[160] Applying this definition to Russia's hacking of the DNC server and its exfiltration and release of internal emails stored on those servers during the run-up to the 2016 presidential election with the

---

[153] Hollis, *supra* note 86.

[154] Schmitt, *supra* note 137.

[155] Hollis, *supra* note 86 ("[M]uch of the debate over the duty of non-intervention has focused on identifying *which* coercive measures below the use of f orce threshold are covered by the prohibition.").

[156] *See* Schmitt, *supra* note 137, for discussion of right of response.

[157] Schmitt, *supra* note 137.

[158] *Id*.

[159] *Id*.

[160] *Id*. The manipulation of election results would also violate sovereignty-as-rule.

purpose of harming one candidate and helping her opponent, Russia's conduct does not clearly qualify as coercive intervention.[161]

A second conception of coercion may be found in the 1970 U.N. General Assembly Declaration on Friendly Relations Among States regarding the duty of non-intervention, which provides: "Every State has an inalienable right to choose its political, economic, social, and cultural systems, without interference *in any form* by another State."[162] If a State's "interference in any form" with another State's right to choose its political system implicates the non-intervention principle, as some scholars have argued, then the broad language used in the Declaration on Friendly Relations would allow the element of coercion in the non-intervention principle to be more readily satisfied.[163] Applying this conception of coercion to Russia's conduct in the run-up to the 2016 presidential election, i.e., the theft and release of the DNC's internal emails designed to affect the choices of the American voting public, would meet the standard for establishing a breach of the non-intervention principle.[164]

For many commentators, two critical inquiries in the coercion analysis as applied to cyber-based information campaigns designed to

---

[161] *Id*. Some scholars have concluded that, though the question is close, Russia's conduct does meet the coercion requirement for purposes of the non-intervention principle, even under the narrower definition of coercion. Schmitt, *supra* note 145, at 8 ("Opinions vary as to whether the cyber operations were coercive in the intervention sense. The emails that were released had not been altered, and it is generally accepted that mere espionage, without more, is not unlawful under international law. The opposing, and slightly sounder, view is that the cyber operations manipulated the process of elections and therefore caused them to unfold in a way that they otherwise would not have. In this sense, they were coercive.").

[162] Declaration on Principles of Int'l Law Concerning Friendly Relations and Cooperation Among States, G.A. Res. 2625 (XXV), Annex, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970) (emphasis added).

[163] *See, e.g.*, Nicholas Tsagourias, *Electoral Cyber Interference, Self-Determination and The Principle of Non-Intervention in Cyberspace*, THE UNIVERSITY OF SHEFFIELD, 1, 14 (2020), http://eprints.whiterose.ac.uk/159652/ (quoting JAMES CRAWFORD, THE CREATION OF STATES IN INTERNATIONAL LAW, 127 (2007)); Hollis, *supra* note 86.

[164] As Professor Duncan Hollis observes, the broader articulation of "interference in any form" provided by the Declaration on Friendly Acts potentially encompasses a wider range of cyber operations targeting the democratic opinion-making of another State's polity, thereby implicating the duty of non-intervention, especially if such operations are "designed to impact public support for . . . an entire 'political' party." Hollis, *supra* note 86. *See also* Barela, *supra* note 8 (arguing for an understanding of coercion that accounts for "[t]he significance and expanse, both in scale and reach, of the interests targeted").

manipulate voting behavior are: (1) whether the information propagated is factually accurate or disinformation; and (2) whether the foreign State is conducting its operations covertly or overtly. If an operation involves disinformation covertly promoted by a foreign State to affect the voting behavior of another State's polity, then "the attempt to manipulate the will of the people" could constitute intervention because it "undermine[s] the target State's sovereign will over its choice of political system" by thwarting the target State's ability to hold free and fair elections.[165] On this view, the deception inherent in disinformation and covert action is key in that it effectively operates as coercion by distorting the electoral discourse and depriving the voting population of the "open democratic space in which to conduct free and fair elections" and, by extension, to decide its political system freely.[166] Absent the deceptive nature of the cyber activity, the foreign State's conduct may be categorized as nothing more than an influence campaign.[167] As one commentator has stated: "In light of the growing frequency of cyber operations implicating the prohibition, further clarification by the international community of the threshold for intervention is badly needed."[168]

B. The Right to Self-Determination

A lesser discussed, but potentially potent, source for assessing the permissibility of foreign-sourced cyber operations, particularly those which attempt to influence a target State's democratic opinion-making, is the right to self-determination recognized under international law. The primary rule for this analysis is the United Nations "Friendly Relations" Declaration, which provides:

---

[165] MOYNIHAN, *supra* note 122, at 41-42; *see also* Kate Jones, *Online Disinformation and Political Discourse: Applying a Human Rights Framework*, 1, 32-37 (2019) (using a human rights framework to argue that "rights to freedom of thought and opinion are critical to delimiting the appropriate boundary between legitimate influence and illegitimate manipulation").

[166] MOYNIHAN, *supra* note 122, at 42.

[167] *Id*. at 42 ("[Official] statements that seek to steer another government's population on a matter may be perceived as propaganda but if they are open and factually correct then they would be less likely to violate the principle of non-intervention because the target state would still have the free will to respond."); Schmitt, *supra* note 145, at 8 ("Coercion is accordingly more than mere influence. It involves undertaking measures that deprive the target State of choice.").

[168] Schmitt, *supra* note 137.

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.[169]

Although a number of commentators view the right to self-determination in connection with the non-intervention principle for purposes of determining breach of international law,[170] at least one scholar, drawing primarily on this provision, contends that self-determination is, standing alone, the proper concept for analyzing cyber operations that employ conspiracy theories and disinformation campaigns propagated by foreign operatives.[171] A key aspect of the self-determination analysis, namely the role of deception in executing the cyber operations, parallels certain core inquiries regarding the coercion element under a non-intervention analysis.[172] Dean Jens David Ohlin explains how Russian operatives, by posing as Americans on social media in an effort to sway [the 2016 presidential] election, deceived American voters, "point[ing] the way to the distinctive harm of this type of election

---

[169] Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States, G.A. Re. 2625 (XXV), Annex, U.N. Doc. A/RES/2625 (Oct. 24, 1970) (emphasis added).

[170] Tsagourias, *supra* note 163, at 13-14 (arguing that "the function of the principle of non-intervention is to protect the principle of self-determination interpreted as the free construction of a state's authority and will" and that accordingly, "external cyber interference amounting to control over the cognitive environment within which such authority and will are formed violates the principle of non-intervention."); MOYNIHAN, *supra* note 122, at 41 ("The right to self-determination, which refers to the right of peoples to determine freely and without external interference their political status and to pursue freely their economic, social and cultural development, is also relevant, and some have noted the link between that right and the principle of non-intervention.").

[171] Ohlin, *supra* note 123, at 1595-1598 (2017) (arguing that the Russian social media campaign violated the right to self-determination rather than the principles of sovereignty and non-intervention); Jens David Ohlin, *Election Interference: The Real Harm and the Only Solution*, CORNELL LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES No. 18-50 (2018), http://ssrn.com/abstract=3276940.

[172] Jens David Ohlin, *Election Interference: The Real Harm and the Only Solution*, Cornell Law School Legal Studies Research Paper Series No. 18-50 at 13 (2018), http://ssrn.com/abstract=3276940 ("[T]he covert nature of the election interference was crucial to its illegality as a violation of the principle of self-determination.").

interference."[173] He argues that this deception enabled "individuals who were not members of the polity" to "fundamentally alter[ ] the political discourse" in the United States.[174] These individuals distorted the political discourse by "gain[ing] inside access to the political process and . . . amplify[ing] [political] viewpoints that . . . were considered marginal and in many cases outside the political mainstream."[175] According to Professor Ohlin, whether the influence campaign changed the outcome of the election is immaterial:

> The particular harm flowed from the fact that the Russians participated in the electoral process while pretending to be Americans. This had a distortionary impact on the electoral process, which is problematic because an election is supposed to articulate the view of the polity, i.e., a fulfillment of that polity's right of self-determination. Once outsiders insert themselves into that process, while pretending to be insiders, the election becomes a function of other-determination rather than self-determination. The election expresses the political will of outside entities rather than the entity that is holding the election.[176]

A major difference the analysis under the self-determination principle standing alone brings to the fore is the pertinent remedy. Election interference by outsiders posing as insiders constituting violations of sovereignty, or non-intervention, gives the affected State certain rights of response. Traditionally, violations of international law accord a right of response in four categories: retorsion, countermeasures, necessity, and self-defense.[177] Retorsion is a punitive or message-sending response taken by a State in reaction to the conduct of another State.[178] This response, some examples of which include the imposition of economic sanctions, the expulsion of diplomats, and the placement of visa restrictions, is considered unfriendly, but it constitutes a lawful reaction.[179] As applied to cyber operations that violate international law, at least one country has stated its position that retorsion may include limiting or severing the infringing State's access to the target State's domestic servers or other infrastructure in its

---

[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*
[177] Schmitt *supra*, note 137.
[178] *Id.*
[179] *Id.*

territory, consistent with any treaty obligations mandating such access.[180] The second category, countermeasures, consist of acts or omissions that, unless taken in response to another State's unlawful actions, would themselves be impermissible under international law.[181] A target State may take countermeasures only in response to an action by another State that is itself impermissible under international law.[182] In addition, countermeasures, which may be cyber or non-cyber in nature, must not be disproportionate to the harm caused by the other State, and they must not violate human rights or obligations under diplomatic law.[183] An example of a countermeasure that a target State may take against an infringing State's unlawful cyber activities is the use of a counter cyber operation to disrupt or shut down the servers, networks, or other infrastructure that the infringing State has used for its unlawful cyber operations.[184] Third, necessity as a response to internationally wrongful conduct by another State consists of an otherwise unlawful action undertaken when it is the only means for safeguarding an essential national interest (such as the power grid, water supply, or banking system) against a grave and imminent danger.[185] A target State may engage in this category of response only when the threat to essential national interest or interests is immediate and the strict conditions for countermeasures cannot be met.[186] The final category, self-defense, authorizes a target State to use force in response to a cyber "armed attack"—that is, a cyber-attack which causes fatalities, physical damage, and destruction akin to a kinetic armed attack.[187] Absent such fatalities, physical damage, or destruction, consensus is lacking about when a cyber-attack qualifies as an armed attack.

These traditional responses, available only after the fact, however, do nothing to vindicate the principle of self-determination, once violated.[188] In other words, "an ex post remedy is no solution at all to an infringement of

---

[180] *Id.* (citing The Netherlands as an example).

[181] *Id.*

[182] *Id.*

[183] Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: An Analysis*, JUST SECURITY (Oct. 14, 2019), https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] Ohlin, *supra* note 172, at 17.

the collective right of self-determination."[189] Accordingly, if cyber activities by foreign governments (or their proxies) seeking to manipulate the voting behavior of another State's polity by posing as members of that polity are deemed to be in violation of the self-determination principle, then the remedy must lie outside the traditional framework of permissible responses for the breach of other international law principles. According to Dean Ohlin, a State subjected to violation of its right to self-determination by the insertion of outsiders into its electoral process, instead of relying on the traditional responses, has but one remedy: real-time exposure of the outsiders and their interference.[190] Only through transparency, that is, only by informing the polity that certain information is being generated or amplified by individuals or entities who are not members of the polity can the target population freely determine the weight and relevance of the information being propagated.

This solution assumes, however, that the insiders who are in power will want transparency—both as to the interfering conduct by outsiders and as to the accuracy of the information being propagated. As the illustrations from Poland's Smolensk conspiracy theory and from the United States' "Stop the Steal" conspiracy theory suggest, however, the very real possibility exists that some government leaders may not want such transparency, especially if the conspiracy theory or disinformation being spread inures to their political benefit.

IV. WHY CLARITY MATTERS AND THE PROBLEMS THAT STATES' SILENCE ENGENDERS

As hostile cyber operations—including the propagation of conspiracy theories and disinformation—proliferate worldwide, clarity in the international law rules governing cyberspace grows increasingly important for at least two broad reasons. First, such clarity establishes the ground rules for the cyber activities that a State may initiate lawfully, thereby promoting stability, predictability, and consistency with respect to what cyber activities are permissible and what activities are impermissible.[191] Clear ground rules function to deter impermissible activities, lower the risk of unintended escalation, and enable robust responses to hostile cyber operations.[192]

---

[189] *Id.*

[190] *Id.* at 15-17.

[191] Michael Schmitt, *Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, JUST SECURITY (Feb. 9, 2017), https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/.

[192] Schmitt, *supra* note 137.

Second, a rules-based world order should expect and indeed require unambiguous legal grounds for a State to be able to invoke a right to respond to a cyber operation.[193] In this regard, clarity concerning the specific elements of consent and coercion is important because these elements form part of the predicate for a targeted State's permissible response options international law.[194]

Despite the need for clarity, certain elements of sovereignty and non-interference remain opaque in the context of cyber-based information warfare.[195] Determining whether cyber operations by a State employing the weaponized use of conspiracy theories and disinformation to manipulate democratic opinion-making in another State violate international law may depend, for example, on whether such operations are analyzed under the principle of sovereignty, the principle of non-intervention, or the principle of self-determination, or on whether the conduct is undertaken covertly or overtly, or, for purposes of a non-intervention analysis, how the element of coercion is defined.[196] Nevertheless, although a few states have taken public positions on how international law applies in cyberspace, most have remained silent.[197]

States' silence on their views concerning how international law applies to cyberspace not only fails to provide the clarity needed for distinguishing permissible cyber activities from impermissible, but it also creates several additional potential problems. First, it depresses the development of international law by failing to acknowledge that a State believes to be an internationally lawful cyber operation or have reacted to what the State believes to be an internationally wrongful cyber operation.[198] The lack of public statements is particularly important when a target State remains silent after becoming the victim of a publicly known cyber operation by an infringing State. In this situation, the target State may in fact launch a response (cyber or otherwise), but that response may be out of public view

---

[193] MOYNIHAN, *supra* note 122, at 4.

[194] Schmitt, *supra* note 137.

[195] *See* discussion *supra* Part II.A.

[196] *See* discussion *supra* Part II.A.

[197] MOYNIHAN, *supra* note 122, at 9-10.

[198] Barela, *supra* note 8 ("Along with jurisprudence, how States react and speak publicly about such activity matters for determining what the law is."); Schmitt & Vihul, *supra* note 123 ("[I]t is essential to be sensitive to customary law's formal components of State practice and *opinio juris* when examining what States do, how they react to actions by other States, and what their officials say publicly.").

and unacknowledged by the target State.[199] In other words, the lack of a visible response does not necessarily mean the lack of an actual response. Nevertheless, as some commentators have argued, a State's secret conduct does not qualify as State practice for purposes of customary international law development.[200] Accordingly, silence hampers the formation and crystallization of customary international law concerning cyber activities.

Second, and relatedly, silence or failure to respond risks creating a potentially false impression of consensus by the international community that particular cyber operations, including practices of information warfare, are internationally lawful and, therefore, risks prematurely crystallizing limitations on permissible actions that target states may undertake in response under customary international law.[201] In other words, because silence may function as a norm-creating force in the development of customary international law, states may be unintentionally contributing to new norms involving cyber behaviors by the mere choice of silence in response to such behaviors.[202] Customary international law has a long history as a primary source of international law, and State practice in the development of international law is of paramount importance.[203] The statute establishing the International Court of Justice as the "principal judicial organ of the United Nations" specifically provides that, in adjudicating disputes, the court shall apply "international custom, as evidence of a general practice accepted as law."[204] As the United Nations International Law Commission

---

[199] MOYNIHAN, *supra* note 122, at 6.

[200] Navarrete & Buchan, *supra* note 123, at 912-14.

[201] Schmitt & Vihul, *supra* note 123, at 1647 (noting that, absent treaty agreements, cyber operations which might currently be impermissible under international law by violating another State's territorial sovereignty could become permissible only if *lex specialis* emerges later through the crystallization of customary international law).

[202] Hollis, *supra* note 86 (posing the following questions relating to Russia's exfiltration and release of DNC emails through WikiLeaks: "[W]hat happens if international law is not invoked and applied to this case? To the extent state practice can involve acts and omissions, might silence suggest that this sort of behavior (hacking and releasing political parties' internal communications) is perceived as lawful (or at least as not internationally wrongful)? In other words, how states react to this case will have follow-on effects on future expectations of responsible State behavior, leading to new norms of behavior in cybersecurity.").

[203] A. Mark Weisburd, *The International Court of Justice and the Concept of State Practice*, 31 U. PA. J. INT'L L. 295, 299 (2009) ("The significance of state practice in international law is difficult to overstate.").

[204] Statute of International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993.

recently reaffirmed, the "existence and content of rules of customary international law" consist of "two constituent elements [which must] be separately ascertained."[205] First is the "requirement of general [State] practice."[206] Second is the requirement "that the general practice be accepted as law (*opinio juris*), mean[ing] that the practice in question must be undertaken with a sense of legal right or obligation."[207] In other words, as articulated by the ICJ in the *North Sea Continental Shelf* cases:

> Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, i.e., the existence of a subjective element, is implicit in the very notion of the *opinio juris sive necessitatis*. The states concerned must therefore feel that they are conforming to what amounts to a legal obligation.[208]

Given that the requirements for "crystallization"—that is, the formal recognition of a rule or principle—of customary international law are State practice and *opinio juris*,[209] and given that the world is in the early days of

---

[205] *Draft Conclusions on Identification of Customary International Law*, U.N. Doc. A/73/10, Y.B. INT'L L. COMM'N, Vol. II, Part Two (2018).

[206] *Id.* This report takes the position that the practice of international organizations may, in some instances, also meet the "general practice" element for determining the existence and content of customary international law but notes that general practice "refers primarily to the practice of States that contributes to the formation, or expression, of rules of customary international law." *Id. See also* Schmitt & Vihul, *supra* note 123, at 1656 ("State practice and expressions of *opinio juris* are obligatory elements of any claim that an obligation to respect sovereignty is legally binding in customary international law.").

[207] *Draft Conclusions on Identification of Customary International Law*, U.N. Doc. A/73/10, Y.B. INT'L L. COMM'N, Vol. II, Part Two (2018).

[208] North Sea Continental Shelf Cases (F.R.G. v. Den.; F.R.G. v. Neth.), Judgment, 1969 I.C.J. 3 (Feb. 20), at para. 77. In this respect, the ICJ also observes that merely because states undertake a certain practice frequently or habitually does not in itself connote a legal duty: "The frequency or habitual character of the acts is not in itself enough. There are many international acts, e.g., in the field of ceremonial and protocol, which are performed almost invariably, but which are motivated only by considerations of courtesy, convenience or tradition, and not by any sense of legal duty." *Id*.

[209] Schmitt & Vihul, *supra* note 123, at 1650, n. 54 ("'Crystallization' of customary international law requires two elements—State practice (*usus*) and the conviction that said practice is engaged in, or refrained from, out of a sense of legal obligation (*opinio juris*)."); Navarrete and Buchan, *supra* at 123, at 911-912.

cyber-based information warfare,[210] the two elements remain underdeveloped as applied to this particular area.[211] Although a few states have taken public positions regarding the application of international law principles to cyberspace, most have not,[212] and even fewer have done so with specific reference to cyber activities employing conspiracy theories and disinformation campaigns.[213]

Finally, silence or failure to respond risks allowing corrupt actors to set the course of customary international law development in the emerging application of international rules to cyberspace, even if only to delay it. In this respect, the role of strategic corruption, that is, corruption "as an instrument of national strategy" is relevant.[214] Strategic corruption occurs when "corrupt inducements are wielded against a target country by foreigners as a part of their own country's national strategy."[215] In an extreme (hypothetical) scenario, a critical mass of State government heads could be bribed, extorted, or otherwise compromised by another State to remain silent and passive in response to cyber-based information-warfare campaigns to sway the behavior of voters in the target states to elect political leaders who will adopt policies favorable to the infringing State or, alternately, to sow distrust in the elections and in democratic governance more broadly.[216] To

---

[210] Harold Hongju Koh, *The Trump Administration and International Law*, 56 WASHBURN L.J. 413, 450 (2017) (observing that "the international law of cyberspace is in its infancy").

[211] Schmitt & Vihul, *supra* note 123, at 1671 ("[P]ractice and *opinio juris* will inform the contours of the rule [of sovereign inviolability] as applied in the cyber context. Over time, it may even contribute to the emergence of *lex specialis* rules that provide for exceptions to the *lex generalis* rule protecting territorial integrity and inviolability."). For a thorough exploration of the still-developing state of international law as applied to cyberspace more generally, see MOYNIHAN, *supra* note 171.

[212] MOYNIHAN, *supra* note 122, at 4-5.

[213] Henning Lahmann, *Information Operations and the Question of Illegitimate Interference Under International Law*, 53 ISRAEL L. REV. 189, 210-212 (2020).

[214] Philip Zelikow et al., *The Rise of Strategic Corruption: How States Weaponize Graft*, FOREIGN AFFAIRS (July/August 2020), https://www.foreignaffairs.com/articles/united-states/2020-06-09/rise-strategic-corruption.

[215] *Id.*

[216] U.S. elections have proven a fertile ground for foreign states to conduct information warfare. In the 2016 U.S. Presidential election, for example, Russia used "[c]yber tools . . . to create psychological effects in the American population," and '[t]he likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the American public about the validity of

the extent that even corruptly obtained silence and inaction in response to such conduct may operate as a normative hydraulic force signaling no disapproval by the targeted states, the infringing State's cyber activities may come to be seen as internationally lawful or at least not wrongful under international law principles.[217]

V. CORRUPTLY OBTAINED SILENCE

In addition to the unsettled international law questions that commentators have identified in the context of cyberspace more generally, this particular scenario (i.e., the silence of government heads corruptly obtained) also raises a number of distinct, but related, issues concerning some of the more granular details of how international law may apply to cyber-based information warfare once the ingredient of domestic cooperation, cooptation, or complicity has been introduced—issues that pertain to the specific elements of consent (in relation to the sovereignty principle) and coercion (in relation to the non-intervention principle), and that, to date, have not been addressed. More particularly, missing from the scholarly and State treatment is the role that corruption, and relatedly, the role of silence, could play in securing consent under the sovereignty principle or in functioning as coercion under the non-intervention principle. This Part identifies some of the relevant questions relating to consent and coercion, with a view toward promoting scholarly inquiry into, and discussion of, the ways in which strategic corruption may distort international law development, particularly as applied to cyber operations that use conspiracy theories and disinformation to manipulate democratic opinion-making.

---

intelligence community reports, and prompting questions about the legitimacy of the democratic process itself." CATHERINE A. THEOHARY, CONGRESSIONAL RESEARCH SERVICE REPORT, INFORMATION WARFARE: ISSUES FOR CONGRESS 10 (Congressional Research Service, 2018). After the election, during his tenure in the Oval Office, Donald Trump routinely promoted conspiracy theories and disinformation to the benefit of foreign adversaries of the United States. Whether he did so as a result of corruption or compromise, or whether he was merely a fellow traveler, remains a matter of speculation. Nevertheless, his willingness to promote the weapons of foreign information warfare, and his repeated refusal even to acknowledge Russia's role, *see*, e.g., Hongju Koh, *supra* note 210, at 452. some plausibility to the extreme hypothetical scenario presented herein.

[217] If not internationally wrongful, then, no State would have a right of response under international law to such conduct. In a less extreme scenario, an infringing State could manage to obtain silence or inaction from less than a critical mass of target states, thereby delaying the formation of an international norm prohibiting the conduct question, but not necessarily creating a countervailing norm.

A. Consent and the Principle of Sovereignty

Separate and apart from the question of whether silence acts as a perhaps unintentional norm-creating force in international law development is the question of whether silence itself can operate as consent.[218] The principle of sovereignty protects a State from territorial intrusions by another State.[219] Breach of the sovereignty principle occurs when the infringing State exerts power in the target State's territory without consent, or interferes with inherently governmental functions of the target State.[220] At the most fundamental level, sovereignty means that a State may make freely its "choice of a political, economic, social and cultural system, and the formulation of foreign policy."[221] Accordingly, a State which conducts activities in another State's territory concerning that other State's inherently governmental functions commits a violation of sovereignty under international law.[222] A target State, however, may consent to such activities by another State, thereby nullifying what would otherwise constitute a violation of sovereignty.[223] The consent exception under the principle of sovereignty raises the question of whether a target State's silence or passivity in the face of otherwise sovereignty-violating conduct by another State can or does operate as implied consent to, or ratification of, the otherwise internationally wrongful activity.[224] Contextualizing the issue more discretely, given the limited scope of this Article, the question becomes whether a target State's silence or failure to respond to a foreign State's use of cyberspace to wage an information warfare campaign consisting of

---

[218] Regarding silence as an unintentional norm creation, see *supra* notes 201–202 and accompanying text.

[219] The Case of the S.S. Lotus (France v. Turkey), Judgment, No. 1, p. 18 PCIJ (series A) (September 7, 1927) (stating that the "first and foremost restriction imposed by international law upon a State is that—failing a permissive rule to the contrary—it may not exercise power in any form in the territory of another State").

[220] Inherently governmental functions "are understood as activity at the very core of state authority, including the activities of the authorities responsible for foreign and military affairs; legislation and the exercise of the police power; and the administration of justice." MOYNIHAN, *supra* note 122, at 15.

[221] Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, Para. 205 ICJ 14. (June 27, 1986).

[222] MOYNIHAN, *supra* note 122, at 15.

[223] *Id.* at 19.

[224] For discussion of the role that silence plays in the international legal framework, see Helen Quane, *Silence in International Law*, 2014 BRIT.Y.B. INT'L L. 240.

conspiracy theories and disinformation for the purpose of affecting voter behavior in the target State effectively constitutes consent.

A host of reasons may explain why a State may opt for silence in this and other contexts,[225] of course, and these considerations arguably weigh against concluding that silence, without more, operates as consent, especially in relation to cyber activities. For example, responses to cyber operations that involve the military may implicate specific "operational concerns" which not only counsel, but indeed require, "a certain degree of reticence . . . to avoid revealing protected information," especially in "emerging areas of warfare."[226] In addition, some silences may result from a State's considered judgment that a binding international rule has not yet crystallized, and such silences reflect nothing more than the absence of an existing norm applicable to the particular situations under scrutiny.[227] Relatedly, silence may signal a position of "strategic ambiguity"[228] wherein a State elects to "refrain from articulating a position while the law develops and the State considers its options for compliance,"[229] perhaps motivated by a desire to retain as much leeway as possible in the cyber realm based upon a belief that binding rules could run counter to the State's own national interests.[230] Finally, a State may choose to remain silent because of "internal disagreement within [that] State" regarding the rights and obligations currently in place under international law.[231] These considerations, one or more of which may account for why states have, at times, publicly proclaimed that certain cyber activity taken by another State breached international law but have declined to identify the specific nature of the international obligation that has been violated, prompt a number of questions.[232] One is whether the reason motivating a State to adopt a posture of silence, in response to another State's cyber operations

---

[225] Ronald Alcala, OPINIO JURIS AND THE ESSENTIAL ROLE OF STATES, ARTICLES OF WAR, LIEBER INSTITUTE WEST POINT (Feb. 11, 2021), https://lieber.westpoint.edu/opinio-juris-essential-role-states/; MOYNIHAN, *supra* note 122, at 9-10; Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, 2018 AM. J. INT'L L. 583.

[226] Alcala, *supra* note 225.

[227] *Id.*

[228] MOYNIHAN, *supra* note 122, at 10.

[229] Alcala, *supra* note 225; MOYNIHAN, *supra* note 122, at 9-10; Efrony & Shany, *supra* note 226, at 588.

[230] Efrony & Shany, *supra* note 225, at 653.

[231] Alcala, s*upra* note 225.

[232] MOYNIHAN, *supra* note 122, at 4 and note 15 (citing example responses from the United States and the United Kingdom to cyber-attacks targeting sites in those states).

targeting it, should have any implications for customary international law development. Another is whether any additional considerations (whether they be supporting or countervailing) come into play regarding a State's silence on the application of international law when those cyber activities propagate conspiracy theories or disinformation aimed at the polity of the target State to affect democratic opinion-making there.[233] As a practical matter, "activities that contravene the non-intervention principle and activities that violate sovereignty will often overlap in terms of outcome."[234] A logical consequence of that relationship may be that consent and coercion also, at times, intersect if not overlap. Accordingly, a separate, but related question is what, if any, are the implications for international law development if a State's silence is deemed to be consent and that silence is rooted in a more nefarious motivation, such as when that silence has been coerced or corruptly obtained by the infringing State. For example, if silence-as-consent has been coerced or corruptly obtained, does the principle of non-intervention become applicable? Relatedly, can silence obtained by corruption operate as coerced consent, and if so, does the coercive nature of the corruption both violate the non-intervention principle and nullify the consent ostensibly granted, thereby also breaching sovereignty?[235]

B. Coercion and the Principle of Non-intervention

As some of the foregoing questions suggest, the principles of sovereignty and non-invention are closely related, and, accordingly, conduct that violates one is likely, in many instances, to violate the other. They are distinct, however, and the primary feature differentiating them is that a violation of the non-intervention principle requires coercive behavior by the infringing State, whereas the sovereignty principle does not.[236] Accordingly, the degree of overlap between the two principles will rest, in part, upon how broad or narrow a definition of coercion is adopted for purposes of the

---

[233] *See* discussion *infra* Part IV.C.

[234] MOYNIHAN, *supra* note 122, at 48; Schmitt & Vihul, *supra* note 123, at 1653 (describing State sovereignty and coercive intervention as related but distinct "prescriptive norms").

[235] This question—though posed here in the specific context of information warfare targeting another State using conspiracy theories and disinformation campaigns—is widely applicable to the questions of consent and coercion in various contexts involving the international legal system more generally.

[236] MOYNIHAN, *supra* note 122, at 48 (citing TALLINN 2.0 MANUAL, para 84 or commentary to Rule 4).

analysis.[237] Assuming, for purposes of this discussion that a broad conception of coercion ultimately crystallizes, the following articulation is useful: "pressure on the victim State to deprive the target of its free will in relation to the exercise of its sovereign powers in order to compel conduct or an outcome with respect to a matter reserved to the target State."[238] On this understanding of coercion, significant overlap exists between the principles of sovereignty and non-intervention in relation to the coercive conduct because such conduct could encompass activity that merely "hamper[s] the target State in . . . the exercise of its sovereign functions in some way," reflecting a close similarity "to the conception of violation of sovereignty as one State's exercise of unauthorized power that usurps the target State's own independent authority . . . ."[239]

In the context of cyber activities the Tallinn Manual 2.0 reflects the international consensus, stating that, "[c]yber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law."[240] In light of the ICJ's recognition in the *Nicaragua* case that the principle of sovereignty encompasses a State's authority to decide freely its "choice of a political . . . system,"[241] international law experts agree that one of the "inherently sovereign functions" of a democratic State is the administration of free and fair elections.[242] If sovereignty is treated not as a standalone rule that itself can be violated, however, then the potential violation must be analyzed under the non-intervention principle. Accordingly, to the extent that a State's cyber operations interfere with the elections of another State—an inherently governmental function which a State is permitted to decide freely—the question becomes whether the cyber activities constitute coercion, thereby breaching the non-intervention principle. More specifically, for the limited purposes of this discussion, the question is whether cyber-based information warfare using conspiracy theories and disinformation to manipulate democratic opinion-making in the target State

---

[237] MOYNIHAN, *supra* note 122, at 48; Ohlin, *supra* note 123, at 1518. ("The concept of coercion can be defined narrowly or broadly, with huge consequences for the outcome of the analysis in this case.").

[238] MOYNIHAN, *supra* note 122, at 48.

[239] *Id.*

[240] Schmitt & Vihul, *supra* note 123, at 1647 (TALLINN MANUAL 2.0, Commentary to Rule 4).

[241] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, 1986 I.C.J. 14, ¶ 205 (June 27).

[242] MOYNIHAN, *supra* note 122, at 40.

qualifies as coercion under the non-intervention principle. The general consensus appears to be yes.[243] As one commentator notes, "[t]he most prominent group of experts writing on cyberwar and cybersecurity has declared that '[i]llegal coercive interference could include manipulation . . . of public opinion on the eve of elections, as when [among other things] . . . false news is spread . . . .'"[244] Another contends that, in addition to "nullif[ying] the genuine expression of authority and will by the people," information warfare that employs disinformation targeting voting behavior "also taints the internal or external manifestation or expression of authority and will by the government that emerges" from the electoral process, thereby violating the principle of non-intervention.[245]

The prevailing analyses, however, presuppose a public response by the target State that seeks to diffuse the effects of any such information warfare on the target polity, either before a given election or afterward. For example, Department of State Legal Adviser Brian Egan, speaking on behalf of the Obama Administration, provided the following public legal interpretation in response to Russia's hack and release of DNC emails during the 2016 election period: "[A] cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention."[246] Similarly, one would expect forceful public pushback against a foreign State that were to remain silent, then the possibility, at least, exists that the target State's silence may be deemed to operate as consent

---

[243] Hongju Koh, *supra* note 210, at 450 (taking the position that "coercive interference in another country's electoral politics—including the deliberate spreading of false news—constitutes a blatant intervention in violation of international law"); Barela, *supra* note 8 (arguing that a foreign power weakening confidence in the legitimacy of a democratic election should be interpreted as an act of coercion); MOYNIHAN, *supra* note 122, at 42 (stating that "[c]oercive efforts to manipulate voting behavior could also amount to intervention in another state's affairs").

[244] Hongju Koh, *supra* note 210, at 450 (quoting TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2d ed. 2017).

[245] Tsagourias, *supra* note 163, at 13-14 (explaining that "the principle of non-intervention protects against external interference the expression of authority and will by the people and also protects the conditions that enable the people to form authority and will freely and make free choices").

[246] Brian J. Egan*, Remarks on International Law and Stability in Cyberspace*, U.S. DEP'T OF STATE (Nov. 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

under the principle of sovereignty,[247] which, in turn, could potentially cast the coercion inquiry under the non-intervention principle in a different light. That is, if the target State, for some reason, acting in its own best interest, adopts silence strategically as an indication of voluntary consent, then the perpetrating State has not acted coercively. However, if the perpetrating State obtains the target State and consequently fails to expose its own polity to the foreign State's interference in the electoral discourse, then perhaps the coercion element should be deemed met.[248]

C. Willing Complicity and Self-Determination

Although the questions that are the focus of this Article relate primarily to strategic corruption as a potential force in the development of international law as applied to cyber activities that use disinformation or conspiracy theories to affect the voting behavior of another State's population, the examples from Poland and the United States of domestic leaders' willingness to use these tactics of information warfare against their own citizens for political gain reveal an additional relevant inquiry: how to address the question of willing, as opposed to coerced, complicity by a target State in actively perpetrating foreign-based conspiracy theories and disinformation campaigns against its own people.

This issue presents even more difficult analytical considerations pertaining to the questions of consent and coercion. At first blush, there would seem to be no violation of sovereignty because consent—in the form of active propagation by instruments of the State—is willingly granted, and the willingness of the grant of consent means the absence of coercion, and therefore, no breach of the non-intervention principle. Considering the issue through the added prism of the right to self-determination, however, may provide a more nuanced analysis.

---

[247] See discussion *supra,* Part IV.A.

[248] Of course, one of the difficulties for international law development in this regard is the public disclosure or exposure of the corruption that would be necessary to apply international law principles to this scenario. Moreover, the questions of what constitutes corruption and how international law treats transnational corruption fall beyond the scope of this Article, but they merit further scholarly attention in the context of malign cyber operations, including information warfare. For a history of anti-corruption features in the international legal system through the Twentieth Century, see Alejandro Posadas, *Combating Corruption under International Law*, 10 DUKE J. COMP. & INT'L L. 345 (2000). For treatment of the more recent problem of strategic corruption, that is, corruption as national strategy employed against a target State, see Zelikow, *supra* note 214.

The principle of self-determination recognizes the collective right of a people to express their independent sovereign will by freely choosing the "political arrangements" that will govern them and the public policy flowing therefrom.[249] International law recognizes this principle in a host of formal instruments. For example, the International Covenant on Civil and Political Rights recognizes "the right and the opportunity" of every citizen "without . . . unreasonable restrictions . . . [t]o vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors."[250] The United Nations Friendly Relations Declaration, under which signatories assume an affirmative duty not to engage in coercive conduct that violates a people's collective rights to self-determination, freedom, and independence, offers another example.[251] When considering these provisions, and others like them, international law experts have opined that the distorted electoral discourse and opinion-making that coalesce under conditions imposed upon a polity by a foreign State's cyber-based information warfare disrupt the legitimate internal processes by which the polity freely chooses its political system and resulting policy and that this disruption deprives the polity of its "capacity to self-determination as self-governance."[252]

An important characteristic of the self-determination principle distinguishing it from the principles of sovereignty and non-intervention is that it is a right that flows not to a sovereign nation but to a sovereign people. Democratic governance is based upon the core notion that the political

---

[249] Ohlin, *supra* note 123, at 1580. ("[S]elf-determination [is] a legal concept that captures the right of a people to decide, for themselves, both their political arrangements (at a systematic level) and their future destiny (at a more granular level of policy.").

[250] International Covenant on Civil and Political Rights art. 25, Dec. 9, 1966, 999 U.N.T.S. 171 (ratified June 8, 1992).

[251] G.A. Res. 2625 (XXV), at annex, State (Oct. 24, 1970) (providing that states have an affirmative duty not to engage in actions that deprive peoples of their rights to self-determination, freedom, and independence).

[252] Tsagourias, *supra* note 163, at 14. ("When a state assumes control over a matter at the expense of the state which has a legitimate claim of authority and will over that matter . . . it effectively curtails the latter's capacity to self-determination as self-governance . . ."); Hongju Koh, *supra* note 210, at 451. ("An external attempt to distort the information that voters possess when they go to the polls also violates the human rights of the electors under the International Covenant on Civil and Political Rights.").

system and its resulting policies represent the will of the people.[253] In a democracy, the people express their "sovereign will" through elections.[254] A foreign State's interference "with the structures and the environment that condition and facilitate the formation of authority and will by the people" works a substitution of "the legitimate process of self-determination with an artificially constructed process in order to generate particular attitudes and results to serve its particular interests" and has the consequence of "control[ling] not only the attitudes, will and choices of the people, but also the will of the government that emerges."[255] Accordingly, a foreign State's use of conspiracy theories or disinformation campaigns to distort and disrupt the target State's electoral discourse and to manipulate the voting behavior therein may be understood as replacing the "sovereign will" of the target State's polity with that of the foreign State.[256] On this understanding, the harm from a State's use of conspiracy theories and disinformation campaigns to affect democratic opinion-making in another State flows primarily to the people of the target State, not to the target State itself.[257] In this way—by

[253] Ohlin, *supra* note 123, 1595. ("The whole point of democratic governance is that the government should represent the will of the people, and this relationship might be called the 'sovereign will.") (distinguishing between the notion of sovereign will of a people as political terminology and the principle of State sovereignty as used by public international lawyers and arguing that the right to self-determination rather than the principle of sovereignty is the appropriate rubric for analyzing election interference targeting democratic opinion-making).

[254] *Id.* at 1595-96 (noting that "[t]he election process is the ultimate expression of a people's sovereign will" and arguing that the Russian government's "illicit interference" with the 2016 presidential election discourse was an effort to supplant the sovereign will of the American people with the sovereign will of the Russian State).

[255] Tsagourias, *supra* note 163, at 16-17.

[256] Ohlin, *supra* note 123, at 1595-96 (2017) (noting that "[t]he election process is the ultimate expression of a people's sovereign will" and that the Russian government's "illicit interference" with the 2016 presidential election discourse was an effort to supplant the sovereign will of the American people with the sovereign will of the Russian state). *See also id*. at 1595-96 (arguing that "[t]he election process is the ultimate expression of a people's sovereign will" and that the Russian government's "illicit interference" with the 2016 presidential election discourse was an effort to supplant the sovereign will of the American people with the sovereign will of the Russian state) and *id*. at 1596 (contending that Russian interference "substituted one sovereign will for the other as an outcome of the election.").

[257] Ohlin, *supra* note 123, at 1596 (arguing that the "relevant victim" of Russia's election interference in 2016 "was not the American State but rather the American people, whose expression of political will was interfered with [sic]").

curtailing the ability of the target State's people to express their sovereign will—the infringing State violates the principle of self-determination.[258]

For commentators who have concluded that self-determination is an appropriate analytical framework for determining the international lawfulness of a foreign State's cyber-based conspiracy theory or disinformation campaigns targeting the democratic opinion-making by the polity of another State, two diverging approaches have emerged, based upon different understandings of the relationship between the principle of self-determination and the principle of non-intervention. One understanding disaggregates the principle of self-determination from the principle of non-intervention and its coercion requirement.[259] This view of self-determination holds that the act of interference itself, without regard to whether or not it is coercive, causes the harm and therefore the violation.[260] The second conception views the right to self-determination as a protection giving rise to the principle of non-intervention.[261] This approach, in other words, would treat the non-intervention principle as an integral component of the right to self-determination:

> By aligning the principles of non-intervention and self-determination, the normative and operational scope of the principle of non-intervention shifts. More specifically, the domain and object of intervention shifts from the government to the actual power holder, the people, and to the process of forming authority and will through which the goal of free choice is also attained. Whereas the government as the depository of such authority and will is protected by the principle of non-intervention, [the State] is not the

---

[258] *Id.* Elsewhere, Professor Ohlin writes:

> An election is supposed to be an expression of that polity's collective will, as a fulfillment of their collective right of self-determination, and outside interference has a distortionary impact on the discourse and threatens to transform what would otherwise be an expression of the polity's will with an expression of some other polity's will.

Ohlin, *supra* note 171, at 15.

[259] Ohlin*, supra* note 171.

[260] *Id.*

[261] Tsagourias, *supra* note 163, at 14. ("When a state assumes control over a matter at the expense of the state which has a legitimate claim of authority and will over that matter because it falls within its sovereign prerogatives, it effectively curtails the latter's capacity to self-determination as self-governance, which . . . [is] protected by the principle of non-intervention.").

> primary object of protection as the traditional reading holds, but a derivative one; the primary object of protection are the people and the process of authority and will formation.[262]

Whether treated as a wholly separate protection or as an adjunct to the non-intervention principle, the right to self-determination would deem a foreign government's utilization of conspiracy theories and disinformation campaigns to deprive the target State's polity of its free choice in exercising its sovereign will as impermissible under international law. Moreover, both approaches also tend to support the view that the willing acceptance and perpetuation by a target State, acting in its sovereign capacity, of a foreign State's cyber activities that weaponize conspiracy theories and disinformation campaigns to manipulate democratic opinion-making in the target State should not operate to nullify protections accorded under the right of self-determination. This is so because the right resides in the people, not in the State.[263] A State's cyber activities used to wage information warfare thus may violate the sovereign will of the target State's polity and, accordingly, violate their right to self-determination, even when the target State's government purports to consent or invite the foreign State's activities.[264]

VI. CONCLUSION

By way of concluding, this Part provides a brief summary and offers recommendations for further study. Current international law framework for addressing cyber operations is adequate. There is no need for cyber-specific rules. The current international law framework consists of multiple principles that could govern determinations of whether particular cyber operations constitute permissible or impermissible activities. Among the most discussed possible applicable principles are sovereignty and non-intervention. A third, less discussed, option is the principle of self-determination. It is yet unclear which of these principles will anchor the analysis, and a number of related subsidiary issues remain unsettled.

---

[262] *Id.*

[263] *See supra* note 253.

[264] Of course, to the extent that a complicit domestic government utilizes or allows foreign-based information warfare against the domestic population, any remedy to which a State might avail itself on behalf of its polity for a violation of the self-determination principle under such circumstances would need to await a new government in the target State, a condition which assumes that the democratic processes retain sufficient vigor to overcome the anti-democratic forces aligned against them.

Regarding sovereignty, international law prohibits the intrusion of a State's territorial integrity, sovereign equality, or political independence by another State. This prohibition may be nullified if a State consents to the intrusion. Disagreement exists as to whether sovereignty is a standalone rule, the violation of which gives rise to a right of response, or whether it is merely a guiding principle, which cannot itself be violated, but which serves both as a channeling function for State action and as the fount for other binding norms, of which one is the principle of non-intervention. If sovereignty is treated as a rule, then its breach may occur by territorial manifestation of foreign State conduct in the target State or by a foreign State's intrusion on the inherent government activities of the target State. Under this framework of sovereignty-as-rule, a foreign State's opinion-influencing cyber operations using conspiracy theories or disinformation to affect democratic electoral outcomes are unlikely to violate the target State's sovereignty under the territorial manifestation prong. Such operations might potentially violate the sovereignty rule under the inherent government activities prong, but this issue remains unclear. If sovereignty treated as only a guiding principle, then such operations cannot violate sovereignty, but must instead be analyzed under other, binding rules that flow from the principle of sovereignty.

One potentially applicable rule is the principle of non-intervention, which prohibits a State from coercively interfering in the inherently governmental functions of another State. Disagreement exists in this area of international law regarding the definition of coercion. Under a narrow definition, a foreign State's cyber-based influence campaigns propagating conspiracy theories and disinformation to manipulate democratic opinion-making in another State's electoral processes do not rise to the level of coercion and therefore do not run afoul of the non-intervention principle. Under a broader definition, however, such conduct could constitute coercion, and the offending State would accordingly be in breach of the non-intervention rule.

The right of self-determination holds that any form of foreign interference, whether direct or indirect, with a sovereign State's internal affairs violates international law. Some commentators view the right to self-determination as inextricably linked with the non-intervention principle for determining such violations, while at least one scholar takes the view that self-determination operates as a stand-alone principle which can be violated when a foreign State launches cyber operations that use conspiracy theories and disinformation campaigns to manipulate the democratic opinion-making of a target State.

Absent treaty agreements governing these types of cyber-based campaigns, customary international law will, over time, likely coalesce and provide answers to at least some of the unsettled questions relating to the various possible principles that could apply to cyber-based disinformation campaigns. To crystallize into binding rules, customary international law requires State practice and *opinio juris*, but a target State's silence or inaction in response to another State's hostile activities can also operate as a norm-creating force in international law, leaving greater leeway for an infringing State to ratchet up the standard for what conduct is sufficiently egregious to warrant a right of response by the target State under international law. To the extent that this is so, international law experts' calls for clarity from states regarding cyber operations should be heeded. In addition to providing clarity on these questions, however, states—and international law experts—would also do well to engage deliberately and prophylactically with a number of peripheral questions concerning the international law implications of State silence, particularly concerning consent and coercion, including questions that address a target State's corruptly obtained silence or passivity in response to the weaponized use of cyber operations to manipulate democratic opinion-making.