ARTICLE

Doxfare:
Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information

Ido Kilovaty*

* Research Scholar; Cyber Fellow, Center for Global Legal Challenges, Yale Law School; Resident Fellow, Information Society Project, Yale Law School; S.J.D. Candidate, Georgetown University Law Center. LL.M., University of California, Berkeley; LL.B., Hebrew University of Jerusalem.

Abstract

Alleged Russian digital interference during the 2016 U.S. presidential election presented international law with the challenge of characterizing the phenomenon of politically motivated leaks by foreign actors, carried out in cyberspace. Traditionally, international law's norm of non-intervention applies only to acts that are coercive in nature, leaving disruptive acts outside the scope of prohibited intervention. This notion raises a host of questions on the relevancy and limited flexibility of traditional international law in relation to new threats and challenges emanating from the use of cyberspace capabilities. The discourse on transnational cyberspace operations highlights how it has become increasingly difficult to deal with nuanced activities that may cause unprecedented harms, such as the hack of the Democratic National Committee, as well as disinformation campaigns on social media, online propaganda, and sensitive information leaks.

This Article argues that state interference with a legitimate political process in another state through cyberspace ought to be considered a violation of the norm of non-intervention. Although the constitutive coercion element is seemingly absent, international law should adapt to the digital era's threats and consider non-coercive interferences that constitute "doxfare"—the public release of sensitive documents with the intent of disrupting legitimate domestic processes—as violations of the norm. As this paper contends, cyberspace operations are distinct in their effects from their physical counterparts, so a traditional standard of coercion for the norm on non-intervention is outdated and requires the introduction of a more nuanced approach, that takes into account interventions that are non-coercive in nature.

Table of Contents

Introduction.....149

I. Doxfare: Covert and Overt Elements 152
A. *The DNC Emails*.....155
B. *The Podesta Emails* 156
C. *Leaky History: Khrushchev's Speech* 157
D. *Weaponization of Information*.....158

II. The International Law of "Doxfare".....160
A. *Non-Intervention*.....161
1. Historical Overview.....162
2. UN Charter, General Assembly, and Group of Governmental Experts Report 162
3. ICJ Jurisprudence 164
4. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.....166
5. Intervention vs. Interference 167
B. *Coercion*.....168

III. A Theory of Intervention for the Digital Era.....169
A. *Doxfare as Intervention* 172

IV. The Challenges Ahead 174
A. *Ungoverned Non-State Actors and the Diffusion of Power*.....174
B. *Countermeasures* 176
C. *Disinformation and Propaganda Campaigns* 178

V. Conclusion 179

Introduction

On July 22, 2016, at the peak of the 2016 U.S. presidential election campaign, WikiLeaks published a series of private emails belonging to the Democratic National Committee (DNC).[1] This leak included nearly 20,000 emails and 8,000 attachments that belonged to seven top officials at the DNC (an event this Article will refer to as the "DNC Hack").[2] While most of the emails were innocuous, a number of them confirmed that the DNC favored presidential candidate Hillary Clinton over Bernie Sanders, causing outrage due to the DNC's professed neutrality regarding the Democratic Party nominee.[3] In the technology community, this type of leak is known as "organizational doxing,"[4] and involves "hackers, in some cases individuals- and in others nation-states, [who] are out to make political points by revealing proprietary, secret, and sometimes incriminating information . . . airing the organizations' embarrassments for everyone to see."[5]

The DNC Hack became a focus of the presidential election and the impetus for an investigation by the Federal Bureau of Investigation.[6] Several U.S. national security officials addressed this as a "national security and counter-intelligence issue."[7] Events subsequent to the DNC Hack included organized protests against the DNC[8] and the resignation of DNC Chairwoman Debbie Wasserman Schultz.[9]

The U.S. intelligence community (IC) released a detailed report in the aftermath of the presidential election as a result of the DNC Hack and other election-related espionage operations involving the distribution of inflammatory

---

[1] Tom Hamburger & Karen Tumulty, *WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, WASH. POST (July 22, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/ [https://perma.cc/4GPY-SDBX].

[2] *Id.*

[3] Michael Shear & Matthew Rosenberg, *Released Emails Suggest the D.N.C. Derided the Sanders Campaign,* N.Y. TIMES (July 22, 2016), https://nyti.ms/2k75jPE.

[4] *See* Bruce Schneier, *Organizational Doxing,* SCHNEIER ON SEC. (July 10, 2015), https://www.schneier.com/blog/archives/2015/07/organizational_.html [https://perma.cc/3SJX-HA8J].

[5] *See* Bruce Schneier, *How Long Until Hackers Start Faking Leaked Documents?* ATLANTIC (Sept. 13, 2016), https://www.theatlantic.com/technology/archive/2016/09/hacking-forgeries/499775/ [https://perma.cc/4YPF-XRHY].

[6] Chris Storhm et al., *FBI Investigating DNC Hack Some Democrats Blame on Russia*, BLOOMBERG (July 25, 2016), https://www.bloomberg.com/politics/articles/2016-07-25/fbi-investigating-dnc-cyber-hack-some-democrats-blame-on-russia [https://perma.cc/8X6F-KJXE].

[7] Duncan 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 [https://perma.cc/69T9-YNSD].

[8] Patrick Healy & Jonathan Martin, *Democrats Struggle for Unity on First Day of Convention,* N.Y. TIMES (July 25, 2016), https://nyti.ms/2Gcpwwf.

[9] Jonathan Martin & Alan Rappeport, *Debbie Wasserman Schultz to Resign D.N.C. Post,* N.Y. TIMES (July 24, 2016), https://nyti.ms/2kTxyT7.

anti-Clinton propaganda on social media. The report concluded that "President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election."[10] Leaders of the U.S. Senate Select Committee on Intelligence endorsed that conclusion, noting that there was a "consensus among members" that Russia was directly involved in the interference operation.[11] This finding largely supported the initial claim made by a cybersecurity firm hired by the DNC that "Russian intelligence-affiliated adversaries" were the entities involved in the intrusion into the DNC network.[12]

The pervasive use of cyberspace for a variety of covert international operations is not surprising, and has been discussed extensively in the literature.[13] In the last few years, states have increasingly used cyber operations to achieve strategic political, economic, and military objectives. Such actions are enabled by common features of cyberspace, which include anonymity, instantaneous cross-border operations, ease of access to the internet, and the low cost of deployment.[14] Cyber-dependent nations are vulnerable to manipulation, disruption, or attacks on their infrastructure, which could shut down political, economic, and social activities.[15]

---

[10] OFF. OF DIR. OF NAT'L INTEL., ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS ii (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/7GTE-5VHJ] [hereinafter IC REPORT].

[11] Karoun Demirjian, *Senate Intelligence Committee Leaders: Russia Did Interfere in 2016 Elections,* WASH. POST (Oct. 4, 2017), https://www.washingtonpost.com/powerpost/senate-intelligence-committee-leaders-russia-did-interfere-in-2016-elections/2017/10/04/1459291c-a91f-11e7-850e-2bdd1236be5d_story.html?utm_term=.8f1015caf2f0 [https://perma.cc/UL7H-TF5F].

[12] *See* Dmitri Alperovitch, *Bears in the Midst: Intrusion into the Democratic National Committee*, CROWDSTRIKE BLOG (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee [https://perma.cc/5SCY-M33E]; *see also* Chris Stokel-Walker, *Hunting the DNC Hackers: How CrowdStrike Found Proof Russia Hacked the Democrats,* WIRED (Mar. 5, 2017), http://www.wired.co.uk/article/dnc-hack-proof-russia-democrats [https://perma.cc/79XJ-67FE].

[13] *See generally* DAVID BETZ & TIM STEVENS, CYBERSPACE AND THE STATE: TOWARDS A STRATEGY FOR CYBER-POWER (2011).

[14] Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L. L. 525, 531–32 (2012).

[15] Paul Cornish, *Deterrence and the Ethics of Cyber Conflict*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS 1, 4 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017) ("[I]t is becoming increasingly difficult to imagine what life was like without social media, email, smartphones, broadband and so on."); *see also* Christopher Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L. L. 825, 826 n.2 ("Stocks are purchased on-line. Applications for employment are made on-line. Work is done on-line. University degrees are earned on-line. Airplane tickets are bought on-line. Communications with friends occur on-line. People even register to vote on-line. The benefits of computer-based Internet system are enormous. Vast amounts of information are literally at the fingertips, facilitating research on virtually every topic imaginable. Financial and other business transactions can be executed almost instantaneously. Electronic mail, Internet websites and computer bulletin boards allow instantaneous communications quickly and easily with virtually an unlimited number of persons or groups.").

Politically motivated leaks by foreign actors are far from new. However, the tactic has been revolutionized by the use of cyberspace.[16] Massive volumes of damaging, sensitive, or classified information can be exfiltrated and released almost instantaneously, a development that challenges notions of sovereignty,[17] non-intervention,[18] and friendly relations.[19] The damage that can be inflicted by leaking sensitive information[20] can be enormous—political processes can be disrupted; fundamental human rights, like privacy and self-determination, can be violated; and the opinions of citizens can be manipulated by the release of materials that a foreign government selects.[21]

The debate on the legal characterization of the DNC Hack was largely indeterminate as it failed to result in an effective characterization of the aggressive action or a response plan.[22] While the debate raised many important arguments about how the international community should treat the politically motivated leaks, it addressed neither the changing nature of foreign intervention nor, most importantly, coercion.[23] For example, according to the IC Report, the purpose of the DNC Hack was to "undermine public faith in the US democratic process."[24] The DNC Hack illustrates a new form of transnational intervention, requiring a reevaluation of what international law should consider as "coercion," a constitutive element of the norm on non-intervention. This Article explores the

---

[16] Ido Kilovaty, *The Democratic National Committee Hack: Information as Interference,* JUST SEC. (Aug. 1, 2016), https://www.justsecurity.org/32206/democratic-national-committee-hack-information-interference [https://perma.cc/CTW4-E4AM].

[17] Sean Watts, *International Law and Proposed U.S. Responses to the DNC Hack,* JUST SEC. (Oct. 14, 2016), https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack [https://perma.cc/BMM5-3M2B].

[18] *Id.*; *see also* Duncan 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 [https://perma.cc/2FPN-MA8N].

[19] Watts, *supra* note 17 ("[A]n emerging view might regard such disruptions to connectivity as unfriendly, but routine and internationally lawful acts.").

[20] I define "sensitive" as any data that is not in the public domain—i.e., an intruder must hack into closed systems to gain (unauthorized) access to the data.

[21] For further discussion on the human rights perspective of the Russian interference, see Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?* 95 TEX. L. REV. 1579, 1583–86, 1594–97 (2017).

[22] *See* Rebecca Crootof, *The DNC Hack Demonstrates the Need for Cyber-Specific Deterrents*, LAWFARE (Jan. 9, 2017), https://www.lawfareblog.com/dnc-hack-demonstrates-need-cyber-specific-deterrents [https://perma.cc/3Y5M-Z38D] (arguing that transposing international law to the cyber realm does not work, calling for a cyber-specific regime, and noting that despite the U.S. response "being the strongest public action the United States has ever taken in response to a cyberoperation, many are bemoaning its inadequacy. The U.S. actions have been derided as 'too little, too late,' 'confusing and weak,' and 'insufficient.' However, this seemingly insufficient reaction may have been informed by international law; the United States might have responded to the DNC hack as it did because international law did not permit it to do more").

[23] Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SEC. (Jan. 5, 2017), https://www.justsecurity.org/35999/international-law-response-russian-election-interference [https://perma.cc/DE65-UV3V].

[24] IC REPORT, *supra* note 10, at ii.

origins and trajectory of the international law norm on non-intervention, while arguing that its coercion component is taking on more nuanced and less physical tones in the digital era, requiring a new layer of legal subtlety if nation states hope to address intervention that is conducted by a phenomenon that I refer to as "doxfare."

Part I of this Article explores the phenomenon of doxfare, which typically comprises three stages: intrusion, publication (or "leak"), and attribution. Doxfare has become a valuable weapon in nation states' offensive arsenals, with a correspondingly marked rise in its deployment.[25] First, this Part will summarize recent massive political leaks—primarily the DNC Hack, which also includes the leak of John Podesta's emails. It will then discuss the famous leak of Soviet leader Nikita Khrushchev's 1956 speech denouncing Stalin, which illustrates that leaking sensitive documents for political gains, while not unprecedented, has taken a new form in recent years with regard to factors like volume and risk. Finally, Part I introduces the phenomenon of "weaponization of information," an expansion of the theory of reflexive control. Part II summarizes the origins and purpose of the norm on non-intervention in international law, outlining the legal framework that should be used to assess the DNC Hack. This includes a deeper look into the precondition that intervention be *coercive* to violate the norm. This historic requirement of international law is the primary hurdle that doxfare must overcome to be considered a prohibited form of intervention. Part III argues for an expanded notion of intervention, taking into consideration the increasing weaponization of information by nation states. Part IV touches on the potential difficulties that could arise from this expanded understanding of intervention, subject to further scholarly inquiry and, perhaps, more informed legal frameworks.

I. Doxfare: Covert and Overt Elements

Doxfare refers to state-sponsored intrusions into foreign computer systems and networks to collect bulk, non-public data that are then leaked for public consumption.[26] Doxfare is a word play on "lawfare," a concept that typically refers to the "strategy of using—or misusing—law as a substitute for traditional military means to achieve an operational objective."[27] Doxfare does not necessarily mean conducting "war" by leaking politically sensitive data, but instead denotes an emerging state practice of conducting foreign affairs by disseminating bulk, non-public information to the public with the intention of influencing the internal or

---

[25] *See* Bruce Schneier, *The Rise of Political Doxing,* MOTHERBOARD (Oct 28, 2015), https://motherboard.vice.com/en_us/article/z43bm8/the-rise-of-political-doxing [https://perma.cc/9QVJ-NGH6]; *see also* Robert Chesney, *State-Sponsored Doxing and Manipulation of the U.S. Election: How Should the U.S. Government Respond?* LAWFARE (Oct. 21, 2016), https://www.lawfareblog.com/state-sponsored-doxing-and-manipulation-us-election-how-should-us-government-respond [https://perma.cc/JZ3B-2ZAR].

[26] *See, e.g.*, Chesney, *supra* note 25 (arguing that "the Russian government has developed a remarkable capacity for blending the fruits of espionage with information operations designed to manipulate public opinion abroad").

[27] Charles Dunlap, *Lawfare Today: A Perspective,* 3 YALE J. INT'L. AFF. 146, 146 (2008).

external affairs of another state. Generally, the norm of non-intervention would protect the victim state from physical intrusions by another state seeking private information.[28] However, cyber-enabled phenomena like doxfare deeply challenge the traditional understanding of what constitutes wrongful "intervention."

As this Article argues, doxfare is comprised of covert and overt elements. Three elements (intrusion, leak, attribution) are required for an act to amount to doxfare and, if sufficiently disruptive, trigger wrongfulness under international law. These three elements are essential to distinguish doxfare from other acts that resemble more traditional intervention, whether cyber-crime or espionage. The covert element is the intrusion into a computer system, which is typically designed to complicate any attempt at attribution.[29] The overt elements are the publication of exfiltrated data, which is usually disseminated on an online platform that allows storage of large volumes of plaintext information, and the subsequent attributional accusations and deflections, which typically include a denial by the suspected culprit.[30]

First, the intruder hacks the computer system by employing one of the common techniques used to compromise a server's software or hardware. The techniques range from social engineering,[31] where the hacker attempts to gain access to the system by stealing the credentials of an authorized user, to actual hacking, where the hacker accesses the system through structural vulnerabilities.

---

[28] *See* Ohlin, *supra* note 21, at 1588 ("When speaking about the general prohibition against interfering with another State's sovereignty, public international lawyers often refer to a State's *domaine réservé*, its exclusive power to regulate its internal affairs without outside interference. Indeed, the notion of *domaine réservé* would seem to be constitutive of the descriptive and normative uses of the phrase 'sovereignty,' in the sense that being a sovereign State naturally entails the power to act as the sovereign. This is the enduring notion of sovereign prerogative.").

[29] *See* Sam Biddle, *Here's the Public Evidence Russia Hacked the DNC – It's Not Enough*, INTERCEPT (Dec. 14, 2016), https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough (claiming that even though the evidence points towards Russian involvement, the evidence is insufficient for attribution).

[30] Andrew Roth, *Russia Denies DNC Hack and Says Maybe Someone 'Forgot the Password'*, WASH. POST (June 15, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/russias-unusual-response-to-charges-it-hacked-research-on-trump [https://perma.cc/CCJ4-WAJ4] ("Over the years, the Kremlin has grown used to brushing off these kinds of accusations.").

[31] *Social Engineering Fraud*, INTERPOL, https://www.interpol.int/en/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud (last visited Nov. 17, 2017) ("'Social engineering fraud' . . . refers to the scams used by criminals to trick, deceive and manipulate their victims into giving out confidential information and funds. Criminals exploit a person's trust in order to find out their banking details, passwords or other personal data. Scams are carried out online—for example, by email or through social networking sites—by telephone, or even in person"); *see also* MALCOLM ALLEN, SOCIAL ENGINEERING: A MEANS TO VIOLATE A COMPUTER SYSTEM 4 (2006), https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529 [http://perma.cc/EN84-6T3M] (defining social engineering as "the art and science of getting people to comply with your wishes").

Typically, these vulnerabilities are imperfections in the code of the operating system or other programs used on the computer.

Second, the "leak" or "doxing" takes place. In this step, the actor behind the data breach publishes that data, usually in bulk, to a platform that hosts these documents. The actor frequently chooses WikiLeaks, an online platform used to host sensitive documents that governments and other actors have attempted to keep out of the public eye. WikiLeaks first gained notoriety for its involvement with the Snowden leaks regarding National Security Agency programs.[32] In January 2017, WikiLeaks marked its tenth anniversary by announcing that it is in possession of ten million unpublished documents.[33] Even though doxfare predates the establishment of WikiLeaks, the platform has made it easier for certain actors to "dump" bulk data, which then becomes available to the public.[34]

Third, once the leak is unleashed, the most likely culprit typically denies complicity and responsibility for the leak. The identity of the perpetrator is nonetheless often established quickly by private cybersecurity firms that compete to rapidly investigate the crime.[35] The relevant authorities of the victim state typically take longer to solidify their evidence and allegations, but the actor (or alleged actor) will continue rejecting these allegations. At times, the perpetrator will deflect responsibility to another actor. In the DNC Hack case, an online persona, named Guccifer 2.0, identifying as a Romanian, announced that it was behind the hack on the DNC.[36] Later, it was found that Guccifer 2.0 is Russian.[37] By denying culpability, the perpetrator attempts to avoid potential legal ramifications and foster chaos and uncertainty in the victim state.

---

[32] *See* Barton Gellman et al., *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.a23939f09437 [https://perma.cc/6WEJ-JKBQ].

[33] *See WikiLeaks Ten Year Anniversary*, WIKILEAKS.ORG, https://wikileaks.org/10years (last visited Nov. 19, 2017) ("WikiLeaks has published over 10 million documents in 10 years, an average of 3000 per day. Each release has shared genuine official information about how governments, companies, banks, the UN, political parties, jailers, cults, private security firms, war planners and media actually operate when they think no one is looking.").

[34] *See* Colin Oldberg, *Organizational Doxing: Disaster on the Doorstep,* 15 COLO. TECH. L.J. 181, 183–84 (2016) (providing several examples of doxing that were not disseminated through WikiLeaks, including the Ashley Madison hack, the Sony Hack, and Snowden's whistleblowing).

[35] *See generally,* 18 U.S.C. § 1030 (2012) (criminalizing unauthorized access and damage to a broad range of computers).

[36] Ellen Nakashima, *Guccifer 2.0 Claims Credit for DNC Hack,* WASH. POST (June 15, 2016), https://www.washingtonpost.com/world/national-security/guccifer-20-claims-credit-for-dnc-hack/2016/06/15/abdcdf48-3366-11e6-8ff7-7b6c1998b7a0_story.html [https://perma.cc/DYP8-2NH6].

[37] Elias Groll, *New Evidence Strengthens Guccifer 2.0's Russian Connections,* FOREIGN POL'Y (July 26, 2016), http://foreignpolicy.com/2016/07/26/new-evidence-strengthens-guccifer-2-0s-russian-connections [https://perma.cc/6G58-JMFL].

A. *The DNC Emails*

The hacks on the DNC computer network occurred during 2015 and 2016.[38] The extent of the strike was first identified by the cybersecurity firm CrowdStrike, which the DNC hired to investigate a possible intrusion into its computer network.[39] CrowdStrike's analysts found two adversaries resident on the DNC's network: "Fancy Bear" and "Cozy Bear," which were previously involved in other cyber incidents, including the infiltration of the unclassified networks of the White House, U.S. Department of State, and other U.S. and international targets.[40]

The sophistication of the hack—and its similarity to the infiltration of other sensitive political targets previously orchestrated by Cozy Bear and Fancy Bear—raised suspicion that a foreign state was involved.[41] In this case, the attack involved a social engineering method of spear-phishing, which targets a specific entity by prompting it to install malicious software. The software then enables selective remote access to the target's computer systems.

Once resident on the DNC computer system, Fancy Bear and Cozy Bear exfiltrated vast volumes of information to other servers, including emails of Democratic Party officials indicating their preference for Hillary Clinton over Bernie Sanders, both candidates for the party's 2016 presidential nomination.[42] In addition, many emails included information pertaining to the party's donors, their credit card details, Social Security numbers, and other personal information.[43] These emails were published on WikiLeaks in two waves, and the timing of each wave appeared strategic. The first batch (20,000 emails and 8,000 attachments) was released on July 22, 2016, days before the Democratic Party Convention in Philadelphia, where there were rumors that already-dissatisfied supporters of Bernie Sanders might attempt to derail the official nomination process. The second batch (8,000 emails) was released on November 6, 2016, the Sunday before the

---

[38] Luke Harding, *Top Democrat's Emails Hacked by Russia After Aide Made Typo, Investigation Finds,* GUARDIAN (Dec. 14, 2016), https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [https://perma.cc/7DMQ-5JTV].

[39] Alperovitch, *supra* note 12.

[40] *Id.*

[41] *Id.* (noting that Crowdstrike, investigating the DNC Hack, "immediately identified two sophisticated adversaries on the network—COZY BEAR and FANCY BEAR. . . . [Their] team considers them some of the best adversaries out of all the numerous nation-state, criminal and hacktivist/terrorist groups [they] encounter on a daily basis").

[42] H.A. Goodman, *WikiLeaks Emails Show DNC Favored Hillary Clinton Over Bernie Sanders During the Democratic Primary*, HUFFINGTON POST (July 23, 2016), https://www.huffingtonpost.com/entry/wikileaks-emails-show-dnc-favored-hillary-clinton-over_us_57930be0e4b0e002a3134b05 [https://perma.cc/2W96-7AMQ].

[43] Joe Uchill, *Exclusive: Hacker Leaks Personal Info of Dem Donors*, THE HILL (Aug. 12, 2016), http://thehill.com/business-a-lobbying/291334-dnc-hacker-leaks-docs-top-dem-donors [https://perma.cc/4HPG-WNA3].

election.[44] Both release dates corresponded closely to known inflection points in the campaign, when public attention was at its zenith and dissatisfied Democrats would be most prone to be affected by negative information about Clinton and the DNC's perceived manipulation of the primary process.

B. *The Podesta Emails*

The DNC was not the only target of the Russian operation.[45] The third batch of emails released by WikiLeaks belonged to John Podesta, the chairman of Clinton's presidential campaign and a former White House chief of staff. The emails were obtained by sending a spear-phishing email to Podesta's Gmail account in March 2016. They were then published on October 7, 2016, a mere hour after the Washington Post released the Access Hollywood tape[46] of Donald Trump making degrading comments about women.[47] The timing of the release—and its favorability to Mr. Trump—reinforced the IC's determination that Russia supported the Republican candidate.

The Podesta emails contained evidence of controversial remarks that Clinton gave to various Wall Street audiences, including Goldman Sachs bankers, lending credibility to the damaging accusation that she maintained a cozy relationship with the financial sector.[48] This leak occurred one day after the White House accused Russia of orchestrating the DNC Hack.[49]

The potentially momentous nature of even the smallest error is demonstrated by the Podesta leak. When Podesta's aide attempted to authenticate the spear-phishing email with the DNC's I.T. personnel, he was told that it was "legitimate," which was revealed to be a typo, as this response also included a

---

[44] Tal Kopan, *WikiLeaks Releases More DNC Emails Near Eve of Election,* CNN (Nov. 6, 2016), http://www.cnn.com/2016/11/06/politics/wikileaks-dnc-emails-surprise [https://perma.cc/MV5W-QK4A].

[45] For the purposes of this Article, the Podesta emails will be considered as an integral part of the overall DNC Hack.

[46] David Fahrenthold, *Trump Recorded Having Extremely Lewd Conversation About Women in 2005,* WASH. POST (Oct. 8, 2017), https://www.washingtonpost.com/politics/trump-recorded-having-extremely-lewd-conversation-about-women-in-2005/2016/10/07/3b9ce776-8cb4-11e6-bf8a-3d26847eeed4_story.html?utm_term=.efa169464f21 [https://perma.cc/3PYX-FW2Y].

[47] Aaron Sharockman, *It's True: WikiLeaks Dumped Podesta Emails Hour After Trump Video Surfaced*, POLITIFACT (Dec. 18, 2016), http://www.politifact.com/truth-o-meter/statements/2016/dec/18/john-podesta/its-true-wikileaks-dumped-podesta-emails-hour-afte [https://perma.cc/WCJ9-MVMY].

[48] Amy Chozick et al., *Leaked Speech Excerpts Show a Hillary Clinton at Ease with Wall Street*, N.Y. TIMES (Oct. 7, 2016), https://nyti.ms/2lsV4nK; Edward Moyer, *WikiLeaks Posts 'Podesta Emails,' Clinton Wall Street Speeches*, CNET (Oct. 8, 2016), https://www.cnet.com/news/hillary-clinton-goldman-sachs-speeches-leaked-paid-wikileaks-john-podesta-julian-assange.

[49] Michelle Meyers, *Russia Deliberately Interfering with Election, US Says,* CNET (Oct. 8, 2016), https://www.cnet.com/news/russia-hacked-dnc-interfere-us-2016-presidential-elections/.

recommendation to change Podesta's Gmail password.[50] The Trump campaign and disenchanted supporters of Sanders used both the DNC and Podesta emails extensively to attack and delegitimize Clinton.[51] These attacks may have swayed the outcome of the U.S. presidential election.[52]

C. *Leaky History: Khrushchev's Speech*

Politically motivated leaks are far from a new phenomenon. The United States was involved in one of the most infamous leaks in modern history when, in 1956, the Central Intelligence Agency (CIA) obtained a copy of Soviet leader Nikita Khrushchev's revolutionary speech denouncing the horrors of Joseph Stalin's reign.[53] At the time, Khrushchev served as the First Secretary of the Communist Party of the Soviet Union.[54] This speech was originally intended for a small group of the Communist Party leadership, but it was made public when Israeli intelligence obtained a copy and passed it on to the Eisenhower Administration.[55] The content of the speech was "unexpected and unprecedented,"[56] as it was a highly classified document not intended for mass media.

After receiving a copy of the speech and consulting with the CIA and Department of State, President Eisenhower agreed to send the speech to the *New York Times*. The tone of the speech, which gave an explicit and unequivocal account of Stalin's atrocities—purges, torture, and political assassinations—set the course for the "de-Stalinization" movement, which was in the interest of the United States.[57]

Although Khrushchev's leaked speech is a kindred example of a politically motivated leak, the DNC Hack should not necessarily be seen as a continuation in the same tradition. First, the volume of documents leaked in the DNC Hack is far

---

[50] Joe Uchill, *Typo Led to Podesta Email Hack Report*, THE HILL (Dec. 13, 2016), http://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack [https://perma.cc/49BY-2X5K].

[51] Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://nyti.ms/2jASgpt.

[52] *See generally* LION GU ET AL., THE FAKE NEWS MACHINE: HOW PROPAGANDISTS ABUSE THE INTERNET AND MANIPULATE THE PUBLIC (2017), https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf?_ga=2.117063430.1073547711.1497355570-1028938869.1495462143 [https://perma.cc/2FDZ-JL9D].

[53] John Rettie, *The Secret Speech That Changed World History*, GUARDIAN (Feb. 25, 2006), https://www.theguardian.com/world/2006/feb/26/russia.theobserver [https://perma.cc/M7Z6-UK2J].

[54] *This Day in History: Khrushchev Elected Soviet Leader*, HIST. CHANNEL (Sep. 12, 2010), http://www.history.com/this-day-in-history/khrushchev-elected-soviet-leader [https://perma.cc/4HEV-KLMT].

[55] Off. of the Historian, U.S. Dep't of State, *Khrushchev and the Twentieth Congress of the Communist Party, 1956*, STATE.GOV, https://history.state.gov/milestones/1953-1960/khrushchev-20th-congress [https://perma.cc/B223-WV3E] (last visited Nov. 19, 2017).

[56] *Id.*

[57] *Id.*

greater than a single speech, potentially multiplying the number of issues that could be "weaponized." Second, the DNC Hack was lower-risk in that a covert intrusion through cyberspace does not expose human intelligence (i.e., spies and informants) to the danger of being caught and turned into counter-intelligence resources by the targeted state. Third, the goals behind these two leaks are different. Whereas with Khrushchev's speech the goal was to highlight Stalin's atrocities, the alleged intention behind the DNC Hack was to cultivate distrust in the democratic system, discredit a political candidate for office, and potentially influence voters to vote for a candidate favorable to the perpetrator's regime.

D. *Weaponization of Information*

The DNC Hack, and its equivalents, create an impression that bulk information is being weaponized. In other words, the leaking of enormous volumes of non-public digital data may have serious consequences that extend beyond the digital realm. These consequences may include criminal investigations, public scrutiny of public officials or government operations, a changed outcome in the political process targeted, and more.

The literature on the weaponization of information focuses on the injection of disinformation and the proliferation of fake news.[58] It is generally accepted that Russia has significantly expanded its budget in these areas over the last few years in order to sway public opinion around the world.[59] The Kremlin's newfound appreciation for the weaponization of information can be found in its reliance on "reflexive control" theory, which offers one compelling explanation of doxfare.[60]

---

[58] *See generally* PETER POMERANTSEV & MICHAEL WEISS, THE MENACE OF UNREALITY: HOW THE KREMLIN WEAPONIZES INFORMATION, CULTURE AND MONEY (2014), https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf [https://perma.cc/8E2G-7ABF].

[59] *See* KEIR GILES, RUSSIA'S 'NEW' TOOLS FOR CONFRONTING THE WEST: CONTINUITY AND INNOVATION IN MOSCOW'S EXERCISE OF POWER 44–46 (2016), https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf [https://perma.cc/V5VM-BHKB]; *see also* David Ignatius, *Russia's Radical New Strategy For Information Warfare,* WASH. POST (Jan. 18, 2017), https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.c1f2ef8d37fc [https://perma.cc/HD7J-5R6Y]; Neil MacFarquhar, *A Powerful Russian Weapon: The Spread of False Stories,* N.Y. TIMES (Aug. 28, 2016), https://nyti.ms/2k6880n.

[60] *See* Annie Kowalewski, *Disinformation and Reflexive Control: The New Cold War*, GEO. SEC. STUD. REV. F. (Feb. 1, 2017), http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war [https://perma.cc/56PT-36WJ] ("Russia's goal is not just to elect a certain candidate in the United States, but to fundamentally undermine the democratic decision-making process to 'win' its information war against the West. Accordingly, Russian disinformation will continue to undermine our political system and act as a direct national security threat to the United States for the foreseeable future."); *see also* Ariel Schwartz, *Cybersecurity Expert: Russian Strategy of "Reflexive Control" Exploited Our Brains in the 2016 Election,* BUS. INSIDER (Apr. 25, 2017), http://www.businessinsider.com/cybersecurity-expert-reflexive-control-2016-election-2017-4; Brandon Valeriano et al., *5 Things We Can Learn from the Russian Hacking Scandal,* WASH. POST

Although the United States and Russia are not in an official state of war, reflexive control may still explain statecraft by doxing.

Reflexive control is the study by one state of an adversarial power to identify and then exploit its weaknesses so as to encourage it to reach a decision that benefits the controlling state. Reflex refers to the "process of imitating the enemy's reasoning or imitating the enemy's possible behavior and cause[ing] him to make a decision unfavorable to himself."[61] The idea is to study the moral, psychological, and personal factors of the target so that those factors can be mimicked or manipulated so as to shape the enemy's perceptions and disconnect them from reality. According to this theory, the side with the "highest degree of reflex (the side best able to imitate the other side's thoughts or predict its behavior) will have the best chances of winning."[62] Reflexive control may be achieved by creating an informational reality of a certain kind (propaganda, leaks, disinformation campaigns), such that one's opponent will *voluntarily* (or, seemingly voluntarily) make a decision favoring the state that created this reality.[63] The decision made by the controlled actor stems directly from the information, or disinformation, communicated to them by the controlling adversary.[64]

Reflexive control theory is gradually becoming a part of a broader phenomenon enabled by the digital era, which allows adversaries to disseminate information that may lead to a strategically desirable outcome. In the pre-cyber era, this was usually achievable only during times of war, where interactions between adversaries were a daily occurrence and geographical proximity allowed the activities associated with reflexive control to take place. Cyberspace empowers reflexive control because it allows the dissemination of information at scale, doing so across political borders, at low cost, and more or less instantaneously. States like Russia, China, and the United States, which each have within their ranks many of the best hackers in the world, are especially well positioned to take advantage of these new circumstances.[65]

(Jan. 9, 2017), https://www.washingtonpost.com/news/monkey-cage/wp/2017/01/09/5-things-we-can-learn-from-the-russian-hacking-scandal/?utm_term=.5c1981733efa [https://perma.cc/G58X-WNZ2] ("Russian operatives, it seems, are once again using the old Soviet tactic of reflexive control, applying it to the cyber era. Reflexive control seeks to manipulate the target to take a position that helps the attacker.").

[61] Timothy Thomas, *Russia's Reflexive Control Theory and the Military*, 17 J. SLAVIC MIL. STUD. 237, 241 (2004).

[62] *Id.* at 242.

[63] *Id.* at 237.

[64] *Id.* at 241.

[65] *See* Reuben Johnson, *Experts: DNC Hack Shows Inadequate Security Against Russian Cyber Attacks,* WASH. FREE BEACON (July 27, 2016), http://freebeacon.com/national-security/experts-dnc-hack-shows-u-s-no-defense-russian-cyber-attacks/ [https://perma.cc/XYJ8-UEE2] ("From around 2007, Russia decided that information warfare was key to winning any world conflict, and that it was this area of capability and technology they decided would benefit from vastly increased military investment . . . . What made this decision easier was that Russia was also home to the largest numbers of some of the world's best hackers.").

Reflexive control theory, although developed by the Soviets in the 1960s[66] and discussed in literature dating back thirty years,[67] appeared in headlines recently in connection to the war in Ukraine.[68] In that context, reflexive control was not purely informational on Russia's behalf; for example, it was reported that Russia concealed and obfuscated its forces (colloquially referred to as "little green men"),[69] publicly denied the real reasons that the Kremlin engaged in war with Ukraine, and shaped the narrative in a way that benefited the Kremlin, primarily by using social media and other online platforms.[70] These actions allowed the Russian government to "create whatever story" it wanted "for whatever audience it want[ed]."[71] Arguably, there is potentially a difference between publishing authentic documents and spreading disinformation or manipulated data, whether that difference is in terms of legitimacy or the degree of wrongfulness under international law.

As states are likely to continue to engage in doxfare in the future, it is essential to examine the international law that could apply to doxfare, namely, the norm on non-intervention.

II. The International Law of Doxfare

International law does not explicitly address data breaches, let alone doxfare, and thus lags behind technological developments and emerging societal trends. Some data breaches may implicate international law norms of general applicability, such as the norm on non-intervention, the inviolability of territorial sovereignty, and, more rarely, the prohibition on the threat or use of force. However, these norms often require a heightened severity of effects in order to distinguish them from legitimate acts of international affairs. For example, the norm on non-intervention requires that an act interfere with the protected internal or external affairs of the victim state, as well as the aggravating element of coercion, targeting the *domaine réservé*[72] of the victim state. It is not always clear

---

[66] Robert Rasmussen, *Cutting Through the Fog: Reflexive Control and Russian Stratcom in Ukraine*, CTR. INT'L MAR. SEC. (Nov. 26, 2015), http://cimsec.org/cutting-fog-reflexive-control-russian-stratcom-ukraine/20156 [https://perma.cc/7TZR-PEFN].

[67] Thomas, *supra* note 61, at 238.

[68] Maria Snegovaya, *'Reflexive Control': Putin's Hybrid Warfare in Ukraine is Straight out of the Soviet Playbook*, BUS. INSIDER (Sep. 22, 2015), http://www.businessinsider.com/reflexive-control-putins-hybrid-warfare-in-ukraine-is-straight-out-of-the-soviet-playbook-2015-9.

[69] *See* U.S. Army Special Ops. Command, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014*, at 31 (2015), http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf [https://perma.cc/XKE8-6XYE] ("Groups of unidentified armed men began appearing throughout the region, often in coordination with local pro-Russian militias. Both the Ukrainian government and most Western intelligence sources claimed that the 'little green men' were Russian operatives.").

[70] *Id.*

[71] Rasmussen, *supra* note 66.

[72] Katja S. Ziegler, *Domaine Réservé*, MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L. L., ¶ 1 http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-

how to apply these notions to a cyber incident that involves data exfiltration, making it immensely difficult to frame some cyber incidents within existing legal instruments.

The most applicable framework for doxfare is the norm on non-intervention because, on a general level, it deals with an act seeking to interfere with a protected internal process of a state. While it is widely accepted that Russia interfered in the U.S. presidential election,[73] commentators have been cautious when considering whether the non-intervention norm was violated.[74] As exemplified in the following sub-part, the traditional understanding of intervention does not conform easily to the emerging role that states are playing in cyberspace, especially when considering theories like reflexive control.

A. *Non-Intervention*

International law prohibits external intervention in the domestic affairs of another state, due to the protective principles of territorial sovereignty and sovereign equality.[75] While this notion appears intuitive, it often poses a major challenge due to its vague and indeterminate nature,[76] including the claim that the principle does not exist at all.[77] Because it is part of customary international law,[78] the principle of non-intervention is sprinkled throughout instruments of international law, with slight variations.[79] The absence of an authoritative and

---

e1398?rskey=qblTRf&result=1&prd=EPIL [https://perma.cc/65LA-AHS6] (last updated Apr. 2013).

[73] *See* Amber Phillips, *8 Times U.S. Intelligence Chiefs Have Unequivocally Said Russia Meddled in the U.S. Election,* WASH. POST (July 6, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/07/06/8-times-u-s-intelligence-chiefs-have-unequivocally-said-russia-meddled-in-the-u-s-election/?utm_term=.df7826e3b175 [https://perma.cc/8SSY-DFYW].

[74] *See, e.g.*, Goodman, *supra* note 23; *see also* Ohlin, *supra* note 21, at 1587; Duncan 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 [https://perma.cc/76G2-P3UF].

[75] *See* U.N. Charter art. 2, ¶ 7; *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep 14, ¶ 251 (June 27) (noting that "[t]he effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of non-intervention"); *id.* ¶202.

[76] *See* Terry D. Gill, *Non-Intervention in the Cyber Context, in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 217, 217 (Katharina Ziolkowski ed., 2013) (providing that "[t]he principle of non-intervention is, on the one hand, a well-established rule of international law and, at the same time, one which is in some respects controversial and open to various definitions and differing interpretations, depending upon how widely or narrowly it is construed").

[77] *See* Anthony D'Amato, *There Is No Norm of Intervention or Non-Intervention in International Law*, 7 INT'L LEGAL THEORY 33, 37–38 (2001) (arguing for a theory of non-intervention limited to efforts to compromise states' territorial integrity).

[78] Nicar. v. U.S., 1986 I.C.J. ¶ 202.

[79] *See* Philip Kunig, *Intervention, Prohibition of*, OXFORD PUB. INT'L L. ¶ 8, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434 [http://perma.cc/C7JP-BZWD] (last updated Apr. 2008).

comprehensive doctrine of non-intervention makes it immensely difficult to apply to actual hostile activities in cyberspace.

1. Historical Overview

One of the earliest iterations of the concept of non-intervention was introduced in 1758 by the Swiss philosopher and legal scholar Emer de Vattel. He wrote that "all these affairs being solely a national concern, no foreign power has a right to interfere in them," and "[i]f any intrude into the domestic concerns of another nation . . . they do it an injury."[80]

Almost forty years later, Immanuel Kant, in his essay *Perpetual Peace*, addressed how governments could achieve and maintain peace while avoiding war. Kant provided that "[n]o state shall by force interfere with the constitution or government of another state."[81] However, as demonstrated during the Holy Alliance period, European governments were not yet ready to adopt the principle.[82]

In 1919, the Covenant of the League of Nations provided one of the earliest codifications of the non-intervention principle. Article 15(8) of the Covenant required that if a "dispute between the parties . . . is found by the [League's] Council[] to arise out of a matter which . . . is solely within the domestic jurisdiction of [one] party, the Council . . . shall make no recommendation as to its settlement."[83] A short time later, in 1933, one of the fundamental instruments of modern international law, the Montevideo Convention, recognized non-intervention as wrongful and provided that "[n]o state has the right to intervene in the internal or external affairs of another."[84] Since then, the most comprehensive adoption of non-intervention has been recognized by the United Nations Charter, and reflected in numerous United Nations (UN) declarations and reports.

2. UN Charter, General Assembly, and Group of Governmental Experts Report

A substantial portion of Article 2 of the UN Charter is dedicated to provisions that internalize the principles of sovereignty and non-intervention, though non-intervention is not explicitly mentioned.[85] Article 2(1) acknowledges that the UN is founded on "the principle of the sovereign equality of all its

---

[80] EMER DE VATTEL, THE LAW OF NATIONS, OR, PRINCIPLES OF THE LAW OF NATURE, APPLIED TO THE CONDUCT AND AFFAIRS OF NATIONS AND SOVEREIGNS 96 (Béla Kapossy & Richard Whatmore eds., Liberty Fund Inc. 2008) (1758).
[81] IMMANUEL KANT, PERPETUAL PEACE: A PHILOSOPHICAL SKETCH § I, art. 5 (1795), https://www.mtholyoke.edu/acad/intrel/kant/kant1.htm [https://perma.cc/8JRA-8QFW].
[82] *See* Kunig, *supra* note 79, ¶ 16.
[83] League of Nations Covenant art. 15.
[84] Montevideo Convention on Rights and Duties of States art. 8, Dec. 26, 1934, 49 Stat. 3097, 165 L.N.T.S. 19.
[85] *See* Gill, *supra* note 76, at 219.

Members,"[86] and Article 2(7) clarifies that the Charter does not authorize the UN to "intervene in matters which are essentially within the domestic jurisdiction of any state."[87] Article 2(4) prohibits what could be described as a "particularly obvious example"[88] of intervention: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[89] Violation of Article 2(4) would constitute a prohibited intervention.[90] Some commentators argue that Article 2(4) cannot address new informational warfare,[91] but scholarship on the matter has focused heavily on how that prohibition applies to cyber-attacks resulting in physical damage, rather than activity that can be categorized as doxfare.[92]

The UN General Assembly further attempted to establish guiding rules on non-intervention in its Declaration on Friendly Relations, which provides that "[n]o State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State"[93] and that "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."[94] The Declaration provides a few concrete examples of intervention, including the organization and encouragement of irregular armed forces and assisting or instigating acts of civil strife or terrorism.[95] Most importantly, however, the Declaration proclaims that "[e]very State has an inalienable right to choose its *political*, economic, social and cultural systems, without interference in any form by another State."[96] The preceding General Assembly Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty contains similar language.[97] Although General Assembly resolutions rarely have

---

[86] U.N. Charter art. 2, ¶ 1.
[87] *Id.* art. 2, ¶ 7.
[88] Nicar. v. U.S., 1986 I.C.J. ¶ 205.
[89] U.N. Charter art. 2, ¶ 4.
[90] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS Rule 66, cmt. 31 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 2.0].
[91] *See* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 112 (2001).
[92] *See* Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SEC. L. 212, 227 (2012).
[93] G.A. Res. 2625 (XXV), annex, at 123, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Oct. 24, 1970).
[94] *Id.*
[95] *Id.*
[96] *Id.* (emphasis added).
[97] *See* G.A. Res. 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (Dec. 21, 1965) ("Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State.").

legally binding force, the International Court of Justice (ICJ) held these particular declarations to reflect customary international law.[98]

Article 5 of the International Law Commission's Draft Declaration on the Rights and Duties of States similarly provides that "[e]very State has the duty to refrain from intervention in the internal or external affairs of any other State."[99] Though still in the drafting process, this document similarly represents widely accepted customary international law on non-intervention.[100]

To clarify the scope of non-intervention in the digital context, the 2015 Report of the UN Group of Governmental Experts reaffirmed that the principle of non-intervention applies to cyberspace and information technologies and, as such, it was incorporated into the rules of responsible behavior in cyberspace.[101] The report provides that "it is of central importance" that "in their use of [information and communication technologies], States must observe . . . non-intervention in the internal affairs of other States."[102] Russia, China, and four other States have gone further by drafting and signing an additional non-binding "international code of conduct for information security."[103] Intervention was not mentioned in this code, but these States pledged "not to use information . . . to interfere in the affairs of other States or with the aim of undermining [their] political, economic, and social stability."[104]

3. ICJ Jurisprudence

As early as 1927, the then-Permanent Court of International Justice ruled in the *Lotus* case that "the first and foremost restriction imposed by international law upon a State . . . [is that] it may not exercise its power in any form in the territory of another State."[105] This is regarded by many as the cornerstone of the modern conception of non-intervention by recognizing the right of independence.[106] In 1949, the ICJ reiterated this idea in its *Corfu Channel* decision,

---

[98] *See* Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention, in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 249, 251–52 (Jens David Ohlin, Kevin Govern & Claire Finkelstein eds., 2015) [hereinafter CYBER WAR: LAW AND ETHICS].
[99] *Summary Records of the 23rd Meeting*, [1949] 1 Y.B. Int'l L. Comm'n 164, A/CN.4/SR.23.
[100] *See* Watts, *supra* note 98, at 252.
[101] *See* Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 at 12 (2015).
[102] *Id.* ¶¶ 26, 28(b).
[103] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, at 4–6, U.N. Doc. A/69/723, annex (Jan. 13, 2015).
[104] *Id.* art. 2(3), at 5.
[105] S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).
[106] Sergio M. Carbone & Lorenzo Schiano di Pepe, *States, Fundamental Rights and Duties*, MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L. L., ¶ 20, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1112?rskey=XsWz2r&result=2&prd=EPIL [https://perma.cc/T92B-HC8G] (last updated Jan.

claiming that it "can only regard the alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to most serious abuses and as such cannot, whatever be the present defects in international organization, find a place in international law."[107]

In its *Nicaragua* decision, the ICJ ruled that "the [non-intervention] principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States."[108] In that case, the Court concluded that the financial support and training provided by the United States to an opposition armed group within Nicaragua was a "clear breach of the principle of non-intervention."[109] The Court explained:

> 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.[110]

The Court also held that non-compliance with the norm of non-intervention does not affect the norm's validity.[111] The Court reaffirmed the principle in *DRC v. Uganda*, applying it to intervention "with or without armed force, in support of the internal opposition within a State."[112]

As much as the principle of non-intervention is a fundamental part of international law, it does not neatly apply to cyberspace in the way that it applies to the physical world, particularly because information is widely available and cyberspace transcends political borders. Recently, the Tallinn Manual has

---

2009) ("What emerges from such authoritative precedents is that, in the absence of a legal norm prohibiting a particular conduct, the right to independence implies the possibility for States to behave freely as members of the international community. To put it differently, one State's right to independence finds its only limit in international norms of customary or voluntary character. Since the world community has not developed as a hierarchic structure, the subjection of States to international law has also to be looked at with particular attention: States, in fact, have a duty to abide by those norms to whose formation they have contributed by concluding (and subsequently ratifying) an international agreement, or which have spontaneously emerged as customary rules."); *see also* Buchan, *supra* note 92, at 222.

[107] Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 35 (Apr. 9).

[108] Nicar. V. U.S., 1986 I.C.J. ¶ 205.

[109] *Id.* ¶ 242.

[110] *Id.* ¶ 205.

[111] *Id.* ¶ 186 ("It is not to be expected that in the practice of States the application of the rules in question should have been perfect, in the sense that States should have refrained, with complete consistency, from the use of force or from intervention in each other's internal affairs.").

[112] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. Rep. 116, ¶ 164 (Dec. 19).

attempted to clarify the complex question of how non-intervention would apply to cyberspace.

4. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

The NATO Cooperative Cyber Defense Centre for Excellence in Tallinn, Estonia, published an updated set of rules derived from international law, as it applies to a broad array of cyber operations, such as espionage, attacks, operations by non-state actors, and more. The Tallinn Manual organizes these rules, which were adopted unanimously by an International Group of Experts (IGE) and represent *lex lata*, the law as (those experts believe) it is, as opposed to *lex ferenda,* the law as it ought to be.[113] As the Manual puts it, ''it is not a 'best practices' guide" and "does not represent 'progressive development of the law.'"[114] In many aspects, the Manual's rules illustrate the myriad inadequacies in the international law applicable to cyber operations. This is also the case with the norm of non-intervention and how the IGE applied it to cyber operations.

The "prohibition of intervention" chapter of the Manual begins with Rule 66, stating that "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[115] The Manual notes that to be prohibited, the intervention must be related to internal or external affairs of a state, it must be coercive,[116] and that even the mere threat of a future intervention violates the norm.[117] The commentary on the rule starts with the acknowledgement that states are realizing the potential of cyberspace to carry out interventions, due to the increasing dependency on information technology and the Internet.[118] The first example of cyber intervention the Manual provides is manipulation of an election by "remotely alter[ing] electronic ballots."[119] This illustrates one of a series of core domestic governmental matters that are susceptible to intervention through cyberspace. The Manual later notes that "the choice of both the political system and its organisation . . . lie at the heart of sovereignty. Thus, cyber means that are coercive in nature may not be used to alter or suborn modification of

---

[113] TALLINN MANUAL 2.0, *supra* note 90, at 2–3.
[114] *Id.* at 3.
[115] *Id.* at 312.
[116] *Id.*
[117] *Id.* at 322.
[118] *See id.* at 312.
[119] *Id.* at 313. Another scenario the Manual gives is "a situation in which one State has two official languages, those of the majority and minority ethnic groups. The government holds a referendum on the dual language policy that results in a decision that only the majority language will remain an official language. A neighbouring State, the population of which is predominantly of the same ethnic background as the minority in the first State, undertakes DoS operations against key governmental websites appearing solely in what is now the official language in an effort to coerce the government into reversing its decision and maintaining websites in both languages. Since a State's language policy in this situation is a matter of its internal affairs, the coercive cyber operations amount to a prohibited intervention." *Id.* at 315.

another state's governmental or social structure."[120] However, even with regard to hacking electronic ballots, which seems to be an easy case, the Manual's experts were split. While the majority of experts believed this to be an act of intervention, because knowledge is not a constitutive element of non-intervention, a few argued that it would only qualify as intervention if the victim state knows of such a cyber operation.[121] This minority view is supported by the claim that the victim state has to know of the pressure exerted against it in order to be effectively coerced.[122]

5. Intervention vs. Interference

Intervention and interference are terms that are often conflated, but "[i]nterference pure and simple is not intervention."[123] This distinction is important. Interference typically implies activities that, although meddling with certain aspects of the internal or external affairs of a state, are not wrongful because they do not involve, for example, coercion or military force.[124] Although documents like the UN General Assembly's Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States seem to disfavor both non-intervention and non-interference,[125] resolutions adopted by the General Assembly do not have a legally binding nature. Despite the ICJ viewing these resolutions as representing customary international law, state practice and opinio juris continue to suggest that non-interference has never actually been adopted as a binding norm.[126]

International law scholars, like Terry Gill, submit that interference "may well be wider than [intervention],"[127] because intervention only includes interference that is "dictatorial" or coercive.[128] Non-coercive acts are therefore mere interferences which are not forbidden by international law.[129] That leads to the question at the crux of this Article: whether coercion is still a reasonable standard to use in determining the lawfulness of states' actions in cyberspace.

---

[120] *Id.* at 315.
[121] *Id.* at 320–21.
[122] *Id.* at 321 ("[T]he minority took the position that coercion includes an element of pressure such that the target State must know that it is being compelled into a particular course of action, that is, the State is acting contrary to its will.").
[123] 1 OPPENHEIM'S INTERNATIONAL LAW: PEACE 432 (Robert Jennings & Arthur Watts eds., 2008) [hereinafter OPPENHEIM'S].
[124] *See* Watts, *supra* note 98, at 255.
[125] *See* G.A. Res 2131, *supra* note 97, arts. 1, 5.
[126] *See* Gill, *supra* note 76, at 224.
[127] *See id.* at 217.
[128] *See id.*
[129] TALLINN MANUAL 2.0*, supra* note 90, at 313 ("States sometimes use the term 'interference' in lieu of 'intervention'. Instruments adopted by States and the UN, as well as judgments of the International Court of Justice, more commonly employ the term 'intervention'").

B. *Coercion*

The requirement of coercion is "the essence of intervention,"[130] yet it is immensely difficult to define the boundary between coercive and non-coercive actions. International law has never officially defined "coercion," nor does it provide any guidance on how this concept is to be construed in cyberspace operations.[131] The ICJ emphasized the centrality of coercion to the notion of non-intervention when it held that "intervention is wrongful when it uses methods of coercion."[132] Certain commentators submit that to constitute a violation of international law intervention must be "forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question."[133] It is also generally accepted that a *threat* of coercion would suffice if it targets the internal or external affairs of a state.[134]

Reliance on coercion as a determining factor means that intervention could only be considered in violation of international law if it reaches a certain degree of severity, and if the coercion pertains to decisions that a state is allowed to make freely as part of its sovereignty, within its "*domain réservé.*"[135] One commentator informally defines coercion as an act of a state against another state to compel the latter "to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force."[136] An indication of coercion could be that the targeted state is undertaking action that "cannot be terminated at the pleasure of the state that is subject to the intervention."[137] The Tallinn Manual clarifies that coercion on its own is insufficient to violate the norm of non-intervention.[138] Commentators note that the intervening act must be "designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State."[139] A few Tallinn Manual experts hold the view that "to be coercive it is enough that an act has the effect of depriving the State of control over the matter in question."[140]

---

[130] Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 348 (2009).
[131] TALLINN MANUAL 2.0, *supra* note 90, at 317.
[132] Nicar. v. U.S., 1986 I.C.J. ¶ 205.
[133] OPPENHEIM'S, *supra* note 123, at 432.
[134] JOHANNN-CHRISTOPH WOLTAG, CYBER WARFARE: MILITARY CROSS-BORDER COMPUTER NETWORK OPERATIONS UNDER INTERNATIONAL LAW 113 (2014).
[135] *See also* Buchan, *supra* note 92, at 223.
[136] Christopher C. Joyner, *Coercion,* MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L. L., http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1749?rskey=qaZy3x&result=1&prd=EPIL [https://perma.cc/ZQJ5-A6CM] (last updated Dec. 2006).
[137] EDWIN DEWITT DICKINSON, THE EQUALITY OF STATES IN INTERNATIONAL LAW 260 (1920).
[138] TALLINN MANUAL 2.0, *supra* note 90, at 318 ("[M]ere coercion does not suffice to establish a breach of the prohibition of intervention.").
[139] *Id*.
[140] *Id*.

One method of determining coercion is "consequentiality,"[141] which considers three factors: "the importance and number of values affected, the extent to which such values are affected, and the number of participants whose values are so affected."[142] While these criteria are helpful in the assessment of coercion, distinguishing between non-coercive and coercive actions is not always straightforward.[143] While the use of military or economic[144] force by one state to persuade another to take a certain path would be a clear-cut case of prohibited intervention, actions in the more subtle environment of cyberspace are more difficult to place on either side of these traditional dividing lines.

In this context, a cyber operation that simply exfiltrates information without using it to coerce the victim state to change the course of its internal or external affairs would not be considered in violation of the norm on non-intervention. It could, however, be a violation of the principle of sovereignty, due to the intrusion into the computer system or network within the territory of the victim state. However, if the exfiltrated information is used in a coercive manner that would most likely trigger the norm on non-intervention.[145]

III. A Theory of Intervention for the Digital Era

The current law on non-intervention is unsatisfactory when applied to doxfare. It ignores the new reality forged by cyberspace, in which information operations are rampant, affecting the outcomes of protected internal or external affairs of the victim state. As such, this Article calls for a reevaluation of non-intervention's application to technically non-coercive but highly disruptive cyber-attacks. In the context of cyber-attacks, I submit that the norm against non-intervention is violated when the attack causes "disruption" rather than outdated notion of "coercion."

Almost thirty years ago, in her seminal work on "Politics Across Borders," Lori Damrosch called for the reevaluation of the norm on non-intervention "as applied to nonforcible efforts to influence another state's internal politics."[146] Damrosch argued that certain transnational political activities are legitimate because they enhance the protection of common international values, such as

---

[141] Myres S. McDougal & Florentino P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War*, 67 YALE L. J. 771, 782–83 (1958).
[142] *Id*.
[143] Lori Fisler Damrosch, *Politics Across Borders: Non-Intervention and Nonforcible Influence over Domestic Affairs*, 83 AM. J. INT'L. L. 1, 4 (1989).
[144] *See generally* Derek W. Bowett, *International Law and Economic Coercion*, 16 VA. J. INT'L L. 245 (1976).
[145] *See* Watts, *supra* note 98, at 256 (noting "a mere intrusion into another state's networks to gather information would certainly amount to a violation of sovereignty. However, without evidence that the effort to gain information formed part of a campaign to coercively influence an outcome or course of conduct in the target state, the intrusion would not be properly characterized as an intervention").
[146] Damrosch, *supra* note 143, at 1.

political participation and, accordingly, reforming non-intervention would ensure that it is in line with recent developments in the concepts of international law as it pertains to individuals and their fundamental rights.[147] However, Damrosch did not address whether such political activities are legitimate when intended solely to promote the standing of the intervening power, while disrupting a legitimate political process in another state and violating notions of political participation and self-determination. More recently, Damrosch admitted that, in the context of the DNC Hack, "[i]t's always been something of a gray area to know what is benign influence in international and domestic politics, and what is prohibited intervention."[148] This seems to suggest that Damrosch's initial argument does not extend to doxfare activities.

The gap in international law related to doxfare is partially due to the rapid evolution of technology vis-à-vis our legal systems.[149] In other words, the principle of non-intervention "fail[s] to keep pace with technological advancements that render territorial limits irrelevant."[150] The implication is that states do not need coercive tools to unduly influence internal or external affairs of another state. International rules should develop in a way that captures these changes.[151] Shifting notions of what constitutes non-intervention are not unprecedented. During the nineteenth century, international law afforded states protection only of their territorial integrity. Not until the twentieth century did the scope of non-intervention expand to protect political independence.[152]

Legal scholarship has begun to hint that the modern conception of coercion—and thus the norm on non-intervention—might need to adjust. For example, Sean Watts reframes coercion in the context of cyberspace. Whether

---

[147] *Id.* at 49 ("[I]n the absence of a valid domestic law to the contrary, influencing states could sponsor programs aimed at strengthening political institutions, assist candidates in obtaining media access, aid political parties through financial contributions or other forms of support, and otherwise exercise political influence not inconsistent with the internationally protected political rights of the target's citizens").

[148] Uri Friedman, *What the DNC Hack Could Mean for Democracy*, ATLANTIC (Aug. 2, 2016), https://www.theatlantic.com/international/archive/2016/08/dnc-hack-russia-election/493685 [https://perma.cc/D3HF-DLVW].

[149] *See generally* Ryan Jenkins, *Is Stuxnet Physical? Does it Matter?*, 12 J. MIL. ETHICS 68, 69 (2013).

[150] Simon Chesterman, *Secret Intelligence*, MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L. L., ¶ 23, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e992?rskey=wEFJF5&result=1&prd=EPIL [https://perma.cc/R9LK-AMAT] (last updated Jan. 2009).

[151] *See* Andrew Fletcher, *Russian Hacking and the U.S. Election: Against International Law?,* 37 MICH. J. INT'L. L. ONLINE (Sep. 29, 2016), http://www.mjilonline.org/russian-hacking-and-the-u-s-election-against-international-law [https://perma.cc/ZU6J-B82P] ("Now countries can possibly disrupt the outcome of other countries' elections without the need for physical coercion. This reality is most dangerous for democracies because elections are the means by which their governments or representatives are chosen. Barring advancements in cybersecurity that would render the issue moot, democracies must establish robust international laws and norms against using cyber-attacks to influence elections.").

[152] WOLTAG, *supra* note 134, at 116.

coercion has occurred in cyberspace, he suggests, should be analyzed based on "the nature of state interests affected by a cyber operation, the scale of effects the operation produces in the target state, and the reach in terms of number of actors involuntarily affected by the cyber operation in question."[153] This approach emphasizes not whether the victim state was *forced* to decide a matter on which it is generally allowed to decide freely, but whether there was an attempt to affect protected state interests and the *effects* that such an operation produces.[154] This would constitute a strong shift from the traditional approach requiring "dictatorial" transnational influence for coercion and thus intervention.[155]

However, voices that support applying existing conceptions of non-intervention to activities such as the DNC Hack without taking into account the unique non-forceful and non-dictatorial aspects of cyber operations miss the point.[156] Though these commentators are making the case that non-intervention applies, there is nearly no analysis of the requirement of coercion, which, if not reevaluated, may pose a challenge in applying the norm on non-intervention to non-forceful and non-dictatorial cyber operations. The notion of coercion does not translate well to cyberspace, because cyber operations can influence and lead to a desired outcome in the victim state without being coercive. Moreover, some commentators argue that coercion in cyberspace must be *secret* to be credible and successful because "discussing or showcasing a [cyber] weapon effectively sacrifices it forever."[157] For example, if State A threatens to carry out a cyber-attack against State B unless State B adopts a decision favorable to State A, then State A takes an immense risk that State B will "respond by hardening systems or even disconnecting them from the Internet." Overt threats of cyber operations thus

---

[153] *See* Watts, *supra* note 98, at 257.
[154] *See id.* at 256–57.
[155] *See id.* at 256.
[156] *See* Steven Barela, *Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion*, JUST SEC. (Jan. 12, 2017), https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion [https://perma.cc/R6MW-S4YR]. Barela argues that foreign actors meddling in election processes, with the intention of delegitimizing them, are committing an act of coercion because "the disruption of a free and fair election strikes at a *sine qua non* for the State." Barela asks whether "disseminating true material can be considered coercion." *Id.* He answers that the Russian hack of the DNC could be considered coercive because releasing the hacked, authentic material was intended to manipulate "public opinion on the eve of elections." *Id. See also* Brian Egan, Legal Adviser, U.S. Dep't of State, Address at University of California-Berkeley School of Law: International Law and Stability in Cyberspace (Nov. 10, 2016), https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf [https://perma.cc/X3YL-B39M] (arguing that "a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention. For increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States' activities in cyberspace").
[157] Craigh Neuman & Michael Poznansky, *Swaggering in Cyberspace: Busting the Conventional Wisdom on Cyber Coercion*, WAR ON THE ROCKS (June 28, 2016), https://warontherocks.com/2016/06/swaggering-in-cyberspace-busting-the-conventional-wisdom-on-cyber-coercion/.

become "useless since the method of entry and exploitation has been eliminated."[158] The non-forceful, non-dictatorial, and secretive nature of cyber operations strengthens the notion that intervention must be re-examined or expanded.

A. *Doxfare as Intervention*

The presence of doxfare can signal an illegal intervention without consideration of coercion. When doxfare significantly disrupts a state's protected internal or external affairs, this disruption should serve as a sufficient substitute for coercion in determining that a wrongful intervention has occurred. This augmented conceptualization of intervention protects the sovereignty of the victim state in a similar way as the existing bar on coercion. The ultimate question is whether a cyberoperation employing doxfare disrupts the protected internal or external affairs of the victim state. The logic behind this is that certain non-coercive acts can still threaten the same values protected by the norm of non-intervention, causing comparable or even greater damage.[159]

Current conceptions of intervention involve an over-reliance on the notion of coercion, which does not necessarily suit the needs and challenges posed by the digital era. For example, the Tallinn Manual distinguishes between "coercion" and "persuasion, criticism, public diplomacy, propaganda, . . . retribution, mere maliciousness, and the like,"[160] which, according to the Manual, are acts of "influencing . . . the voluntary actions of the target State, or seek no action on the part of the target State."[161] This, however, does not address doxfare, which is not coercive *per se*, but inherently includes more than State A having influence over State B. Although the Tallinn Manual gives a few relatively easy scenarios that do not qualify for the non-intervention principle, a few drafters claimed context and consequences of an act are required to determine whether a violation occurred.[162] This disagreement is present in one example from the Manual: State A leaks the domestic intelligence records of State B to create a political crisis within the victim State B,[163] with the result that State B adopts a policy that it would not have adopted otherwise. Drafters were split on whether State B's action was caused directly by the leak and was therefore coerced.[164] Without explicit coercion, it is debatable whether intervention occurred.

In contrast, a disruption-based analysis accounts for highly consequential interferences in the cyber realm that may have been non-coercive. Doxfare that

---

[158] *Id*.
[159] *See* Friedman, *supra* note 148 (arguing that "[i]t follows almost like a syllogism that non-forcible techniques that are equally intrusive should be equally prohibited. But because those techniques are so diffuse, it's much harder to see any bright lines").
[160] TALLINN MANUAL 2.0, *supra* note 90, at 318.
[161] *Id*. at 319.
[162] *Id*.
[163] *Id*. at 320.
[164] *Id*.

causes severe disruption, for example, would be independent proof of intervention and the violation of non-intervention norms. Doxfare is, in many respects, a form of political sabotage carried out through cyberspace, with the purpose of disrupting an ongoing internal or external process that is integral to one of the host of matters upon which a state is allowed to decide freely.[165] Not every information leak will be a wrongful intervention because some form of consequentiality must attach to it to be wrongful, as noted by McDougal and Feliciano.[166] It is therefore argued that doxfare constitutes an illegal intervention when the internal or external process is successfully disrupted by a foreign power acting within cyberspace, and the victim state suffers severe domestic or international consequences. The full range of factors that may determine whether an instance of doxfare is wrongful due to the severity of its disruptive effects will have to be further developed through state practice and evaluated on a case-by-case basis. This is particularly true in a rapidly developing technology context, where adversaries could potentially use new technologies in ways that circumvent traditional understanding of what constitutes an internationally wrongful act.

In the aftermath of the DNC Hack, I have argued that intent and invasiveness can, in addition to severe disruption, help to determine whether doxfare occurred at a level that was wrongful.[167] Intent is already considered by many to be a constitutive element of the norm on non-intervention.[168] Some commentators submit that intent is not relevant, and that coercion is the primary constitutive element of intervention.[169] Given that cyberspace operations may not be immediately identified and analyzed for what they are,[170] and that inadvertent

---

[165] *See* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. 1, 7 (2017) ("These are matters that international law leaves to the sole discretion of the State concerned, such as the 'choice of a political, economic, social and cultural system, and the formulation of foreign policy.' To illustrate, elections fall within the *domaine réservé*, such that using cyber means to frustrate them would raise issues of intervention. By contrast, purely commercial activities typically do not. Therefore, a State's cyber operations that are intended to afford business advantages to its national companies would not amount to intervention. Between these extremes, the scope of *domaine réservé* is indistinct. For instance, States generally enjoy an exclusive right to regulate online communication in the exercise of its sovereignty. Yet, the point at which international human rights law, such as the rights to freedom of expression or privacy, takes domestic regulation beyond the confines of the *domaine réservé* remains unsettled.")

[166] McDougal & Feliciano, *supra* note 141, at 782.

[167] *See* Kilovaty, *supra* note 16.

[168] TALLINN MANUAL 2.0, *supra* note 90, at 321.

[169] *See* Watts, *supra* note 98, at 268–69.

[170] *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L. SEC. L. & POL'Y 63, 64 (2010) (noting that cyber-attack and exploitation are almost identical technically and that "[t]he primary technical difference between cyber-attack and cyberexploitation is in the nature of the payload to be executed—a cyber-attack payload is destructive whereas a cyberexploitation payload acquires information nondestructively. In addition, because a cyberexploitation should not be detected, the cyber operation involved must only minimally disturb the normal operating state of the computer involved. In other words, the intelligence collectors need to be able to maintain a clandestine presence on the adversary computer or network despite the fact that information exfiltrations provide the adversary with opportunities to discover that presence").

outcomes of regular cyberspace activities could happen,[171] intent is a critical factor when identifying internationally wrongful doxfare. Intent may distinguish between acts that are actual interventions, as opposed to acts that just *appear* to be interventions, but have no interventionist purpose.[172]

Invasiveness is another factor that should be considered when identifying wrongful doxfare, since it could indicate the resources—in terms of time, knowledge, and money—invested by the perpetrator to mount the doxfare operation. This may assist in determining the severity of the interference and whether this is a prohibited intervention or an allowable interference. Invasiveness is very much the difference between a hostile act—in which actual hacking takes place, penetrating into an IT system that holds the sought-after data—and other forms of benign activities, such as requesting the information directly through the acceptable channels.

International law conceptions of intervention should be reevaluated to address non-coercive but highly disruptive cyber-attacks. I argue that the norm against non-intervention is violated when one state commits a highly disruptive cyber-attack against another. Such an attack, which I call doxfare, violates the norm against non-intervention even when the attack does not meet outdated notions of "coercion." Doxfare can be identified by the attack itself as well as the intention behind the attack and its level of invasiveness. With the addition of doxfare, the norm of non-intervention is violated when one state attempts to coerce another or when one state commits doxfare against another.

IV. The Challenges Ahead

Labeling disruptive doxfare as a violation of international law's norm on non-intervention is one step towards a more restricted cyberspace playing field. However, it also presents new challenges in application. This part addresses three of the most difficult applications of doxfare: non-state actors who engage in doxfare, the retaliatory countermeasures regime, and disinformation and propaganda campaigns with an interventionist intent.

A. *Ungoverned Non-State Actors and the Diffusion of Power*

International law traditionally applies to affairs between states and, recently, also between states and individuals under international human rights law. This means that non-state actors are generally unbound by international law.

---

[171] *See e.g.*, Dimitar Kostadinov, *The Attribution Problem in Cyber Attacks*, INFOSEC INST. (Feb. 1, 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref. [https://perma.cc/86VY-XC3U] (noting that "[c]ivilians may also inadvertently launch a cyber-attack").

[172] For an opposing view, see Watts, *supra* note 98, at 268–69. For a discussion in the economic coercion context, see William Mattessich, *Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage*, 54 COLUM. J. TRANSNAT'L. L. 873, 880–81 (2016).

Coupled with the idea of diffusion of power, this creates a danger of non-state actors engaging in cyber operations and even more threatening activities in cyberspace without being governed by international law. As one commentator puts it, "[n]ear instant global communications . . . can place very small amounts of power in the hands of enormous numbers (billions) of people" and "place enormous financial, criminal and even destructive power in the hands of a very small number of technologically skilled people."[173]

This diffusion of power means that states no longer have a monopoly over cyberspace, and more non-state entities are becoming involved in cyberspace activities on a large scale.[174] This diffusion challenges the conceptual underpinnings of international law, which assumes that international law applies and is relevant primarily to states because states are its creators and enforcers.[175] Joseph Nye aptly summarized it by saying "[a]nyone from a teenage hacker to a major modern government can do damage in cyber space."[176] While states will remain the dominant actor on the world stage, they will find the stage far more crowded and difficult to control with the continued growth of non-state activity in cyberspace.[177] Of course, states who hire the services of hackers or armed groups to attack another state will still be accountable and responsible for an internationally wrongful act.[178] The crucial gap for international law would be

---

[173] Paul Cornish, *Deterrence and the Ethics of Cyber Conflict*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS 1, 4 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017).

[174] JOSEPH S. NYE, JR., CYBER POWER 1, 4 (2010), https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf [https://perma.cc/F5SJ-F76D] ("States will remain the dominant actor on the world stage, but they will find the stage far more crowded and difficult to control. A much larger part of the population both within and among countries has access to the power that comes from information. . . . [T]he barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost. In contrast to sea, air and space, 'cyber shares three characteristics with land warfare—though in even greater dimensions: the number of players, ease of entry, and opportunity for concealment. . . . On land, dominance is not a readily achievable criterion.' While a few states like the United States, Russia, Britain, France, and China are reputed to have greater capacity than others, it makes little sense to speak of dominance in cyber space as in sea power or air power. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors.").

[175] *See* Kubo Mačák, *Is The International Law of Cyber Security in Crisis?*, *in* 8TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: CYBER POWER 127, 139 (N. Pissanidis, H. Rõigas, & M. Veenendaal eds., 2016), https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf [https://perma.cc/KBM6-BZC6] ("What matters is whether, and to what extent, states will reclaim their traditional central legislative role. Their conduct in the next few years will determine whether we will observe a gradual demise of inter-State governance of cyberspace or a fundamental recalibration of legal approaches with states taking centre stage once again. If they want to ensure that the existing power vacuum is not exploited in a way that might upset their ability to achieve their strategic and political goals, states should certainly not hesitate too long.").

[176] NYE, *supra* note 174, at 9.

[177] *Id.* at 1.

[178] *See* Int'l Law Comm'n, Rep. on the work of its 53rd Session, U.N. Doc. A/56/10, at 47–49, 91–94, 124–25 (2001) [hereinafter Draft Articles on Responsibility] (Articles 8, 31, and 47 of the

when non-state groups act on their own behalf to carry out powerful cyber operations that rise to the level of doxfare.

This may be resolved, in part, by applying the principle of due diligence. The principle provides that even if a state was not complicit in an internationally wrongful act by non-state actors residing in its territory, the victim state could still demand that the harboring state take reasonable measures to stop the act. The principle, in other words, requires that states not allow the use of their territory to carry out cyber operations against other states.[179] This principle dates to the *Corfu Channel* decision, in which the ICJ ruled that states are under an obligation "not to allow knowingly [their] territory to be used for acts contrary to the rights of other States."[180] In addition, better international cooperation and threat-intelligence sharing may prevent and deter potential non-state attacks.[181]

B. *Countermeasures*

The legal regime of countermeasures allows a victim state to respond to an internationally wrongful act with many possible retaliatory tools.[182] Countermeasures represent "measures that would otherwise be contrary to the international obligations of an injured state vis-à-vis the responsible state, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[183] Countermeasures are problematic in the context of cyberspace because certain prerequisites could prevent the victim state from responding to a violation in real-time, and also the risk of escalation could dissuade retaliatory action. Even if the international community characterizes doxfare as a wrongful act, it will not necessarily clarify the enforcement and retaliation questions inherent in cyberspace.

Certain commentators argue for countermeasures in the form of "active defenses" that attempt to target and neutralize the source of a cyber-attack. Such countermeasures are problematic because they can lead to escalation.[184] Although countermeasures must be proportionate and necessary in relation to the initial

---

commission's Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries).

[179] TALLINN MANUAL 2.0, *supra* note 90, at 30 ("A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.").

[180] U.K. v. Alb., 1949 I.C.J. at 22.

[181] *See generally* Nicolo Bussolati, *The Rise of Non-State Actors in Cyberwarfare*, *in* CYBER WAR: LAW AND ETHICS, *supra* note 98, at 102, 102–26.

[182] *See* Draft Articles on Responsibility, *supra* note 178, arts. 1–3, at 32–38.

[183] *See id.* at 128.

[184] Oona A. Hathaway, *The Drawbacks and Dangers of Active Defense*, *in* 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 39, 40–41 (P. Brangetto, M. Maybaum,, J. Stinissen eds., 2014), https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2014.pdf [https://perma.cc/3HPY-L8VN].

internationally wrongful act,[185] they still require identifying the perpetrator and ensuring no harm is caused unrelated to the initial cyber-attack.[186] This typically comprises a two-step determination: (1) whether the act was an internationally wrongful act, and (2) whether this internationally wrongful act could be attributed to a state.[187] While this paper argues that doxfare *may* be considered a violation of the norm on non-intervention, it is difficult to establish in every case that a state orchestrated the act.[188] There is also a concern that these countermeasures may not even be effective enough to induce compliance with international law, a fundamental requirement of the regime of countermeasures.[189]

Another substantial challenge in applying countermeasures to a doxfare analysis is that the injured state is legally required to ask the responsible state to cease its violation[190] and to inform the latter of any countermeasures the former intends to undertake.[191] However, the countermeasures regime recognizes that, sometimes, urgent countermeasures are required and therefore allows them more or less instantaneously.[192] These urgent countermeasures are susceptible to overuse in the cyberspace context, due to the rapid and unexpected nature of cyber operations, further raising the risk of escalation.[193]

The challenges of ineffective countermeasures and fear of escalation may be partially mitigated by "[c]ollaboration between technical experts and international lawyers"[194] that will ensure non-escalatory measures in response to any violation of the norm on non-intervention. Also, better cooperation between states and law enforcement authorities globally could ensure peaceful means of

---

[185] *See* Draft Articles on Responsibility, *supra* note 178, arts. 51–52, at 134–37.
[186] *See* Hathaway, *supra* note 184, at 47.
[187] *See* Draft Articles on Responsibility, *supra* note 178, art. 2, at 68.
[188] *See* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L. L. ONLINE 11, 17 (2011) ("[In the context of the Estonia cyber-attacks,] the apparent wrongfulness of the attacks themselves does not establish that Russia was their 'author.' Attribution is notoriously difficult in the cyber-context, and the Estonia case is no exception. Initial claims that the Russian government coordinated the attacks quickly gave way to intimations that it (at most) tacitly supported the civilian perpetrators. Such circumstantial evidence is treacherous ground upon which to base countermeasures, as a state would be fully liable for any error in judgment.").
[189] Hathaway, *supra* note 184, at 46–47.
[190] *See* Draft Articles on Responsibility, *supra* note 178, art. 52(1)(a), at 135.
[191] *Id.* art. 52(1)(b), at 135 ("Before taking countermeasures, an injured State shall . . . notify the responsible State of any decision to take countermeasures and offer to negotiate with that State.").
[192] *Id.* art. 52(2), at 135 (providing that an "injured State may take such urgent countermeasures as are necessary to preserve its rights").
[193] *See* Hinkle, *supra* note 188, at 18 ("[T]he nature of cyber-force weighs in favor of an injured state resorting rapidly, and with broad discretion, to countermeasures. Because cyber-attacks are often both unexpected and capable of significantly impairing critical infrastructure, they are more likely to be viewed as 'emergency scenarios' justifying reasonable state discretion in employing countermeasures.").
[194] *See* Hathaway, *supra* note 184, at 50.

dispute resolution are given priority over forceful responses.[195] This would not necessarily solve the fundamental complexity of the law on countermeasures in the context of cyberspace and doxfare, and perhaps an adaptation to cyberspace would eventually be inevitable.

C. *Disinformation and Propaganda Campaigns*

Doxfare is not a broad enough concept to include disinformation and propaganda, both of which are on the rise in cyberspace. These are sometimes referred to as "subversive interventions"[196] by a state, such as propaganda "with the intention of influencing the situation in another State."[197] This might be a prohibited intervention if it seeks to interfere in the domestic or external affairs of a state by inviting civil strife or possibly armed conflict. However, the challenge is that disinformation campaigns and propaganda will become pervasive, resulting in dissemination of false information, and possibly leading to dangerous scenarios. Companies like Facebook, Google, and Twitter have already come under fire recently for not combatting the Russian disinformation campaigns on their respective platforms, a phenomenon that is often labelled "fake news."[198] However, fake news is not necessarily sufficient to qualify as doxfare, since it does not necessarily result from leaks or hacks. In the future, fake news may become more sophisticated and nuanced, and pose some serious conceptual challenges to what is considered prohibited intervention.

Reflexive control theory teaches us that interventions may be subtler and more strategic than we would anticipate. This could further suggest, even if doxfare is illegal under the norm of non-intervention, that states will find other methods of influencing each other's internal or external affairs. Propaganda and other sophisticated disinformation campaigns may become the new form of intervention. Devoid of coercion or disruption components, such activities would be outside the scope of the non-intervention norm, both as that norm is construed currently and as this Article argues it should be modified to capture phenomena like doxfare. States are likely to adopt certain norms on cyberspace conduct, though disagreements may persist. At this point, international law does not have a clear doctrine on disinformation and propaganda, and further development of state practice would be required.

---

[195] Ido Kilovaty & Itamar Mann, *Towards a Cyber Security Treaty*, JUST SEC. (Aug. 3, 2016), https://www.justsecurity.org/32268/cyber-security-treaty/ [https://perma.cc/475U-55GG] (arguing that adapting the Chemical Weapons Convention model to cyberspace might mitigate many of the threats we are facing today as "such a treaty will advance cyber-peace and cooperation between states").

[196] *See* Kunig, *supra* note 79, ¶ 24.

[197] *Id.*

[198] Hamza Shaban et al., *Facebook, Google And Twitter Testified on Capitol Hill. Here's What They Said*, WASH. POST (Oct. 31, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/31/facebook-google-and-twitter-are-set-to-testify-on-capitol-hill-heres-what-to-expect/?utm_term=.8d6a125abb30 [https://perma.cc/N2ZF-AS9C].

V. Conclusion

Cyberspace allows humanity to communicate, trade, research, and share information on a global scale. This increased interdependence comes at the cost of increased threats and legal-political challenges that cannot be easily resolved.[199] This Article expands the existing conception of intervention to argue that interference through cyberspace, even when lacking a coercive element, may still be wrongful. Such interference may be doxfare—that is, state-sponsored massive doxing of politically sensitive and confidential information. As demonstrated in this Article, the absence of coercion does not mean that a cyber operation is not interfering unduly with the internal or external affairs of the victim state. Expanding intervention to include disruptive doxfare remedies this limitation.

Treating disruptive doxfare as a prohibited intervention will solve part of the problem with harmful transnational cyber activities, though some second-order questions will require further development, particularly questions of attribution, enforcement, and countermeasures. However, there is substantial value in labeling certain harmful cyber operations as prohibited interventions as this might raise the price-tag associated with possible violations. International law is very much a creation of states, which reach consensus on certain contentious legal issues. It is ultimately up to states to secure a robust multilateral agreement on the rights, duties, and boundaries of state activity in cyberspace.

---

[199] *See* Joyner & Lotrionte, *supra* note 15, at 826 ("[T]he technology-intensive Information Age brings with it opportunities for 'cyber-crime', 'cyber-war' or, as more aptly put, the prosecution of 'information Warfare.'").