BEYOND BALLOT-STUFFING: CURRENT GAPS IN INTERNATIONAL LAW REGARDING FOREIGN STATE HACKING TO INFLUENCE A FOREIGN ELECTION

LOGAN HAMILTON*

Propaganda is to a democracy what the bludgeon is to a totalitarian state.[1]

ABSTRACT

A state actor hacking and releasing information for the purposes of influencing another country's democratic election process is an unprecedented event that has not yet been analyzed under international law. Currently defined areas of "cyber law" are inadequate for describing the phenomena, and existing international law has few proscriptions against such behavior. Given the increasing importance of digitization and "cyber law" in international law, a proposed framework for a treaty addressing this issue will provide states an ideal to work towards.

---

* Logan R. Hamilton will receive his J.D. from the University of Wisconsin Law School in May 2018. Before attending law school, he earned a B.A in History from the College of William & Mary. Logan would like to thank: his family for their continued support; Professor Heinz Klug for his invaluable advice as the faculty advisor to the Wisconsin International Law Journal; and the Wisconsin International Law Journal Senior Editorial Board for assistance throughout the writing process.

1 NOAM CHOMSKY, MEDIA CONTROL: THE SPECTACULAR ACHIEVEMENTS OF PROPAGANDA 16 (Greg Ruggiero & Stuart Sahulka eds., 2d ed. 1997).

INTRODUCTION

In July 2016, approximately nineteen thousand emails and several thousand other internal documents from the Democratic National Convention ("DNC") were released on WikiLeaks, and an additional batch was later released to The Hill.[2] A hacker (or collection of hackers) calling itself "Guccifer 2.0," hacked the DNC and obtained the documents before later releasing the documents.[3] The release of the cache coincided with the Democratic nomination convention and resulted in the resignation of the DNC's chairwoman.[4] The effects of the information release can still be felt through fierce, continuing coverage of the DNC, the Democratic Party, and the former presidential candidate, Hillary Clinton.

US intelligence agencies are increasingly convinced that the hack was not the work of an independently operating "Guccifer 2.0."[5] Instead, intelligence agencies and security experts believe that Guccifer

---

[2] 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/; Joe Uchill, *Guccifer 2.0 releases new DNC docs*, HILL (July 13, 2016, 12:43 PM), http://thehill.com/policy/cybersecurity/287558-guccifer-20-drops-new-dnc-docs.

[3] Reuters, *'Lone Hacker' Claims Responsibility for Cyber Attack on Democrats*, NBC NEWS (June 16, 2016, 7:08 AM), http://www.nbcnews.com/tech/tech-news/lone-hacker-claims-responsibility-cyber-attack-democrats-n593491.

[4] Jonathan Martin & Alan Rappeport, *Debbie Wasserman Schultz to Resign D.N.C. Post*, N.Y. TIMES (July 24, 2016), http://www.nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html?_r=2.

[5] David E. Sanger & Eric Schmitt, *Spy Agency Consensus Grows That Russia Hacked D.N.C.*, N.Y. Times (July 26, 2016), http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.

2.0 is employed by at least one intelligence organization of the Russian government.[6] On October 7, the Department of Homeland Security and Office of the Director of National Intelligence released a joint statement alleging that "the Russian Government directed the recent compromises of e-mails from US persons and institutions."[7] This statement went on to further affirm that the US believes "the Guccifer 2.0 online persona [is] consistent with the methods and motivations of Russian-directed efforts."[8] The motivation for this hack and info dump has been assumed to be the Russian government's intent to influence the course—and outcome—of the 2016 US presidential election, with the goal of electing Donald Trump as President of the United States.[9] Admittedly, it would be naïve to assume that states have never interfered in other states' elections before, even within the U.S.[10] It is, however, the digital *hacking*, particularly of a non-governmental organization, and the subsequent release of the stolen information to influence another state's election, that appears to be new.[11]

In Section II, this note will examine and attempt to define the main areas of "cyber law" that relate to state behavior and understanding

---

[6] 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/.

[7] DEP'T OF HOMELAND SEC., JOINT STATEMENT FROM THE DEPARTMENT OF HOMELAND SECURITY AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE ON ELECTION SECURITY (2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[8] *Id.*

[9] *See id.*; David E. Sanger & Nicole Perlroth, *As Democrats Gather, a Russian Subplot Raises Intrigue*, N.Y. TIMES (July 14, 2016), http://www.nytimes.com/2016/07/25/us/politics/donald-trump-russia-emails.html; Adam Entous & Ellen Nakashima, *FBI in Agreement with CIA that Russia Aimed to Help Trump Win White House*, WASH. POST (Dec. 16, 2016), https://www.washingtonpost.com/politics/clinton-blames-putins-personal-grudge-against-her-for-election-interference/2016/12/16/12f36250-c3be-11e6-8422-eac61c0ef74d_story.html.

[10] For example, money from the Axis powers was used to attempt to influence U.S. politics in 1938. Evan C. Zoldan, *Strangers in a Strange Land: Domestic Subsidiaries of Foreign Corporations and the Ban on Political Contributions from Foreign Sources*, 34 L. & POL'Y INT'L BUS. 573, 576 (2003). For several other relevant examples of foreign states attempting to interfere in U.S. elections, see Lori Fisler Damrosch, *Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs*, 83 AM. J. INT'L L. 1, 15 n.48, 22 nn.82–83 (1989).

[11] The JOINT STATEMENT explained that "[s]uch activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there." DEP'T OF HOMELAND SEC., *supra* note 7. Recent developments in Europe, however, seem to validate this assessment, based on a variety of similar occurrences. *See* Editorial Board, *Russian Meddling and Europe's Elections*, N.Y. TIMES (Dec. 19, 2016), https://www.nytimes.com/2016/12/19/opinion/russian-meddling-and-europes-elections.html.

of cyber law, specifically "cyber espionage," "cybercrime," and "cyber-attacks." Section II will also explore whether such definitions are capable of adequately explaining hacking to release information to influence another country's elections. From there, this paper will propose a new category of "cyber law," specifically "cyber covert action." In Section III, this note will examine the applicability of current international law to the problem of cyber covert actions by states. This note will argue that neither the UN Charter nor customary international law can apply to such actions or provide a remedy to impacted states. Next, the note will argue that while domestic law can apply to cyber covert actions, such law fails to provide appropriate remedies. In Section IV, this note will examine the problem of attribution, which must be noted and accounted for in any effective cyber treaty. This section will then examine Professor Muir's proposed Trilateral Cyber Treaty and explore the intricacies and benefits of such a cyber treaty. Finally, this note will conclude by proposing a series of modifications to the cyber treaty to make the proposed cyber treaty more applicable to cyber covert actions.

I. BACKGROUND

A. HISTORY OF INTERNATIONAL CYBER LAW

International "cyber law" is a relatively new field of law, which has been primarily focused on the military implications of "cyberwarfare" and how to analogize "cyber law" to physical terms. Cyberspace and "[t]he Internet [are] . . . by-product[s] of the science and technology race of the Cold War."[12] Given the decentralized and multi-national nature of cyberspace's physical infrastructure[13] and the transmission of electronic data, cyberspace may be fairly categorized as international space.[14] As such, "[a]ctivity in cyber space . . . must comply with the relevant international law."[15] As a result, international legal scholars have only seriously approached the issue of cyber law since the mid-1990s.[16] However, given the Cold War origins of cyberspace,[17] much

---

[12] Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 527 (2012).

[13] Such physical infrastructure includes "cables, wires, and routers" required to keep cyberspace up and running. Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 323 (2015).

[14] *See* Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17 J. CONFLICT SECURITY L. 187, 189 (2012).

[15] *Id.*

[16] *Id.* at 187 n.1.

legal scholarship regarding cyber law has been in the context of "cyberwarfare." This militarized way of thinking was further crystallized from cyber law's early beginnings as "most of the international law scholars working on cyber security questions from the early days of the Internet were in the military or had close ties to it."[18]

The initial development of scholarship surrounding cyberwarfare seemed to address the question of whether the conventional laws of war applied. Scholars grappled with the brand-new nature of cyberspace, the militarized thinking of previous generations of scholars, and the abstract nature of information as a weapon. Indeed, "[m]any difficult questions ar[ose] when trying to fit cyberspace within a warfare regime constructed long before even the most visionary policy makers imagine[d] cyber weapons."[19] Thus, "[s]ome have posited that the law of war only applies to cyberwarfare by analogy."[20] However, legal scholarship seems to have since coalesced around the idea that conventional laws of war are still applicable to cyberwarfare, notwithstanding some specialized difficulties. The "problems generated by cyber attacks are often similar to the problems of conventional attacks. The differences between conventional and cyber warfare are of degree, not of kind."[21] Despite the existence of a scholarly paradigm from which to understand cyberwarfare, to this day, states and international organizations have still failed to create any "treaty provisions that directly deal with 'cyber warfare.'"[22]

Currently, states and international law scholars generally recognize that a state's cyber activities can fall under the laws of war.[23] Under the United Nations Charter, "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[24] This

---

[17] *See* Jordan Peagler, *The Stuxnet Attack: A New Form of Warfare and the (In)Applicability of Current International Law*, 31 ARIZ. J. INT'L & COMP. L. 399, 403–04 (2014).

[18] O'Connell, *supra* note 14, at 199.

[19] Gervais, *supra* note 12, at 579.

[20] Peagler, *supra* note 17, at 409.

[21] Gervais, *supra* note 12, at 579.

[22] N. ATL. TREATY ORG., COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 5 (Michael N. Schmitt ed., 2013), https://ccdcoe.org/tallinn-manual.html [hereinafter TALLINN MANUAL].

[23] *See generally* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 427–28 (2011); *Tallinn Manual*, *supra* note 22, at 45–52.

[24] U.N. Charter art. 2, ¶ 4.

prohibition does not apply to a state acting in self-defense against armed attacks.[25] Crucially, the "U.N. Charter fails to outline what constitutes 'use of force' in cyberspace."[26] Traditionally, "the dominant view . . . has long been that the Article 2(4) prohibition of use of force and the complementary Article 51 right of self-defense appl[ies only] to military attacks or armed violence."[27] This recognition is exemplified by Russia's proposal, in the late 1990's, of a treaty to ban "espionage and the use of malicious code in cyber conflict."[28] This was opposed by the United States on the grounds that it would inhibit "the United States' ability to [militarily] defend itself in a cyber conflict."[29]

International scholars, and states, recognize as well that cyber activities may indeed rise to the level of a use of force per Article 2(4) or an armed attack per Article 51.[30] Generally, "[t]he laws of war provide the framework for when it is acceptable to resort to the use of force (jus ad bellum) and governs the limits of acceptable wartime conduct (jus in bello)."[31] Applying this body of international law to how states manipulate and interact with packets of data required additional interpretational schemes by scholars. Scholars have proposed three main schemes for attempting to analyze cyber activities under the current international laws for war: instrumentality,[32] target-based,[33] and consequentiality.[34] The instrumentality approach appears to be ill-favored by scholars as it either precludes cyber activities on the basis of not involving purely physical force or requires all cyber activities to be

---

[25] U.N. Charter art. 51, ¶ 1 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.").

[26] Peagler, *supra* note 17, at 411.

[27] Waxman, *supra* note 23, at 427.

[28] Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 905 (2012).

[29] *Id.*

[30] *See* Waxman, *supra* note 23, at 427.

[31] Gervais, *supra* note 12, at 535.

[32] The instrumentality (or method) approach analyzes the delivery method of the attack. *Id.* at 538.

[33] The target-based "approach holds that a cyber-attack rises to the equivalent of . . . use of armed force whenever it penetrates the critical infrastructure of a nation." Peagler, *supra* note 17, at 410–11. This, of course, requires a determination of whether the infrastructure is considered "critical" by the impacted nation.

[34] The consequentiality approach evaluates the impact of the cyber activity and whether the activity results in the same effects as an armed attack would. *See id.* at 411.

treated as using force.[35] Similarly, the target-based approach is disfavored as it "introduces interpretive difficulties by collapsing the distinctions between armed violence, coercion, and interference . . . [and] would authorize self-defense for the most benign offenses."[36] The consequentiality approach is the favored approach as it focuses on the *consequences* of any cyber-attack, such as whether "the effects of a cyber-attack are equivalent to those produced by a traditional attack."[37] For despite their non-physical nature, cyber activities can lead to real world consequences, such as "major disruption of critical infrastructures . . . [in which] lives are lost and property destruction is widespread, [and which] would lead reasonable observers to conclude the effects or results of the information operations exceed the Article 51 threshold."[38] This mode of analysis is considered the predominant view among scholars for "determining whether a hostile cyber act constitutes an armed attack."[39] This work is complicated, however, by the fact that the technical means by which states conduct cyber activities are very similar, whether for espionage or cyberwarfare, and thus are nearly indistinguishable until after the fact.[40]

Scholarship into international cyber law in regards to cyberwarfare became particularly relevant following cyber-attacks on Estonia in 2007 and Georgia in 2008.[41] Following the Estonia attacks, NATO established an "Internet defense facility in Estonia, called the Cooperative Cyber Defense Centre of Excellence (CCDCOE)."[42] Given the uncertainties still surrounding international law and cyberwarfare, the CCDCOE, in 2013, released the Tallinn Manual. The Tallinn Manual was the product of a multi-year effort by leading international law scholars to "identif[y] the international law applicable to cyberwarfare

---

[35] *See generally* Gervais, *supra* note 12, at 537 (noting that "treating all forms of cyber attack as a use of force would require an implausibly broad reading of Article 2(4) that includes non-physical damage").

[36] *Id.* at 538.

[37] Peagler, *supra* note 17, at 411; *see* Gervais, *supra* note 12, at 539–40.

[38] Daniel J. Ryan et al., *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1181 (2011).

[39] Jack M. Beard, *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law*, 47 VAND. J. TRANSNAT'L L. 67, 115 (2014).

[40] *See* Aaron P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations*, 111 MICH. L. REV. 423, 425 (2012).

[41] *See* O'Connell, *supra* note 14, at 192–94.

[42] *Id.* at 193.

and set[] out ninety-five 'black-letter rules' governing such conflicts."[43] This manual seems to represent the first steps towards creating a coherent international body of law regarding cyberwarfare. Similarly, the 2001 Convention on Cybercrime represents a step towards coherently creating, not merely transposing, an body of international law in regards to cyberspace, even though the Convention addresses only non-state actors committing "cybercrimes."[44]

B. HISTORY OF THE NORM OF NON-INTERVENTION

A state-actor hacking to release information to influence another state's elections also implicates the international norm of non-intervention. The custom of non-intervention has a long history and has been "accepted as customary international law, binding on all states."[45] This principle has also been explicitly stated in UN resolutions, ICJ court cases, and individual treaty obligations.[46] The principle has also been validated by Latin American states and regional treaty organizations.[47] As discussed above, the principle of non-intervention has traditionally concerned the usage of physical, armed force against another state.[48] However, "despite the frequency of . . . [the norm of non-intervention's] incantation in international discourse, how the norm applies in nonforcible conduct is inadequately understood,"[49] especially in regards to cyber activities.

---

[43] TALLINN MANUAL, *supra* note 22, at intro.

[44] *See* EUR. CONSULT. ASS., CONVENTION ON CYBERCRIME (2001) [hereinafter the Budapest Convention].

[45] Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 443, 495 (2015). Somewhat ironically, "Russia generally maintains a hyper-formalist, positivist approach to international law, including arguing against evolving customary doctrines" although such an approach is belied by some of Russia's justifications for intervening in the Ukrainian territory of Crimea. *See* Boris N. Mamlyuk, *The Ukraine Crisis, Cold War II, and International Law*, 16 GER. L.J. 479, 491–92 (2015).

[46] Lotrionte, *supra* note 45, at 493–96 ("As additional authority for the principle of non-intervention, the Court invoked the Corfu Channel case, other General Assembly resolutions, including the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, and inter-American practice.").

[47] Damrosch, *supra* note 10, at 7.

[48] *Id.* at 3 ("[T]he prevailing viewpoint until well into the 20th century was that the international legal concept of intervention concerned itself only with the use or threat of force against another state and not with lesser techniques.").

[49] *Id.* at 1.

To counter this, legal scholarship has expressed alternative views of what might constitute "force" or "armed attack" under this regime in terms of cyber activities. "Just because a cyber-attack or cyber espionage do not amount to an armed attack does not mean that international law has no law against such wrongs. Interference . . . even if not prohibited by treaty is prohibited under the general principle of non-intervention."[50] One such alternative view of Article 2(4) and 51 "reads [their] purpose more expansively and looks not at the instrument used but its general effect: that it prohibits coercion."[51] This approach has seemingly been endorsed by the Tallinn Manual, which as the first step towards international cyber law, acknowledges that:

> 10. Cyber operations falling below the use of force threshold are more difficult to characterize as a violation of the principal of non-intervention. Acts meant to achieve regime change are often described as a clear violation. So too is coercive 'political inference.' When such actions are taken or facilitated by cyber means, they constitute prohibited intervention. Cases in point are the manipulation by cyber means of elections or of public opinion on the eve of elections. . . . As always, the decisive test remains coercion. Thus, it is clear that not every form of political or economic interference violates the non-intervention principle.[52]

A related approach attempts to understand force as interference in the state. As posited by scholars, their analysis "would focus on the violation and defense of rights—specifically, a state's right of sovereign dominion."[53] This approach offers an effective means of analysis as "[s]uch an approach ties the concept of force to improper interference with the rights of other states, focusing on the object and specific character of a state's actions rather than a narrow set of means or their coercive effect."[54] This line of analysis also has some support in international courts as the "ICJ has referred to some of this conduct as 'less grave forms' of force that violate the principle of non-intervention while not triggering rights of a victim State under Article 51."[55] This allows states to claim violations of their national sovereignty, yet does not fully implicate Article 2(4).

---

[50] O'Connell, *supra* note 14, at 202.

[51] Waxman, *supra* note 23, at 428.

[52] TALLINN MANUAL, *supra* note 22, at 45.

[53] Waxman, *supra* note 23, at 429.

[54] *Id.*

[55] O'Connell, *supra* note 14, at 202–03.

C. HISTORY OF COVERT ACTION

In terms of covert action, international law is largely underdeveloped, especially so in relation to cyberspace. It is important to specify the terminology, specifically "covert action" and how it differentiates from "espionage." These two terms are legally differentiable. Cyber espionage is "a deliberate cyber action that seeks to extract confidential information from . . . [a] computer system or network . . . without the user's knowledge,"[56] whereas covert action is "conduct that is officially unacknowledged by the responsible state, reflecting secrecy on the narrow issue of attribution" and which includes "unacknowledged operations intended to influence events in another country, conducted by any state agency or actor, or other entity acting on behalf of a state."[57] This definition of covert action is "largely consistent with but slightly broader than the U.S. statutory definition of 'covert action.'"[58] The commonalities between these two definitions show a consistent understanding between states and scholars into how to interpret whether an activity is a 'covert action.'

Since states have existed, states have engaged in activities against one another.[59] Currently, "there are no treaties or customary norms that explicitly proscribe the practice" of covert action,[60] much less covert action in cyberspace. "International law neither prohibits covert conduct per se nor exempts it from legal purview."[61] In 1927, the Permanent Court of International Justice in *Turkey v. France* (the *Lotus* case) held that states may act, except where such actions are affirmatively prohibited.[62] As such, covert action, while permitted, "must comply with the requirements of international humanitarian law."[63] Since the *Lotus* case, "[l]egal scholars often take a fatalist position on the

---

[56] Gervais utilizes the term "cyber exploitation," but largely within the same context as "cyber espionage." The author feels that it appropriate to utilize Gervais' definition given the context. *See* Gervais, *supra* note 12, at 533.

[57] Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507, 511–12 (2015).

[58] *Id.* at 512 (citing and comparing the U.S.'s National Security Act's definition of covert action); *see* 50 U.S.C. § 3093(e) (2012).

[59] Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1162 (2011).

[60] *Id.* at 1165.

[61] Perina, *supra* note 57, at 527–28.

[62] *See* S.S. Lotus (Fr. v. Turk.), Judgement, 1927 P.C.I.J. (ser. A) No. 10, at 21 (Sept. 7).

[63] Williams, *supra* note 59, at 1180.

phenomenon of intelligence gathering."[64] Given the long historical precedent and vital state interests involved, scholars "mostly conclude that covert action must be taken for granted"[65] as an activity that states would engage in regardless of its legality. Importantly, as well, states nearly always "criminalize these [covert] activities from a defensive standpoint."[66] Overall, covert action's legality may be conceptualized as "regulated by international law to the extent it amounts to coercive interference into the affairs of another state or the nonconsensual exercise of state powers on the territory of another state."[67]

Ultimately, "the more consequential the impact on the foreign state, the more likely it constitutes intervention violating that state's sovereignty."[68] As a result, "it seems likely that a cyber intrusion that requires the manipulation of cyber assets in a foreign state through hacking or otherwise, does constitute an exercise of extraterritorial state power"[69] and thus a violation of non-intervention affecting the state's sovereignty. However, it is worth noting, as discussed above, that "acts of espionage and acts of political . . . coercion within the scope of Article 2(4)" have been purposefully omitted from international law by states.[70] Furthermore, although there is no specific mechanism for dealing with cyber covert action, international law already has pre-existing mechanisms which can be repurposed for analyzing cyber covert actions.

II. THE LACK OF AN INTERNATIONAL LEGAL PARADIGM TO FULLY UNDERSTAND RUSSIA'S ACTIONS

In Section II, this note will examine and attempt to define the main areas of "cyber law" that relate to state behavior and understanding of cyber law, specifically "cyber espionage," "cybercrime," and "cyber-attacks." This section will, concurrent with defining such activities, explore whether such definitions are capable of adequately explaining

---

[64] Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICH. J. INT'L L. 687, 692 (2007).

[65] *Id.*

[66] Williams, *supra* note 59, at 1164.

[67] Craig Forcese, *Pragmatism and Principle: Intelligence Agencies and International Law*, 102 VA. L. REV. ONLINE 67, 80 (2016).

[68] *Id.* at 81.

[69] *Id.* at 80.

[70] *See* Jack M. Beard, *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law*, 47 VAND. J. TRANSNAT'L L. 67, 118 (2014).

hacking to release information to influence another state's elections. This section will conclude that the traditional definitions of such areas of "cyber law" are not adequate for the purposes of a meaningful analysis. Rather, a new category of "cyber law," specifically "cyber covert action," that examines the intent and actions of such cyber activities is required to enable meaningful analysis.

A. CYBERCRIME

For the ordinary user, cyberspace opens a world of possibilities in regards to education, entertainment, and improving everyday life. For criminals, cyberspace has proven to be a realm of near-endless possibilities for profit and mischief. With increases in cyberspace interconnectivity by populations and governments, governments have begun to pay more attention to combatting cybercrime. Despite this increased focus, there is no legal and internationally recognized definition of what constitutes an international cybercrime.[71] The Budapest Convention does not attempt to *define* what precisely constitutes a cybercrime, but instead merely lists types of criminal offenses that fall under the Convention.[72] Instead, a more complete definition of cybercrime may be characterized as criminal offenses where the computer or its information is the target, otherwise traditional criminal offenses (e.g. fraud, money laundering, etc.) conducted through cyberspace, or some combination thereof.[73]

Even with this broad definition of cybercrime, this paradigm fails to allow for any meaningful analysis regarding when a state hacks in order to influence another state's elections. Principally, utilizing cybercrime as a template for analysis fails because cybercrime is predicated on domestic investigation and prosecution, even for international crimes.[74] Investigation and prosecution imply that the acting state has jurisdiction or, at the very least, the ability to impose its punishment on the offender. Yet, a state hacking and releasing information to influence another state's election would either not be subject to the prosecuting state's jurisdiction or could ignore the

---

[71] Nicholas W. Cade, *An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code*, 37 BROOK. J. INT'L L. 1139, 1144 (2012).

[72] *See* Budapest Convention, *supra* note 44, arts. 2–10.

[73] *See* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 10 INT'L J.L. & INFO. TECH. 139, 144–46 (2002).

[74] *See* Budapest Convention, *supra* note 44, at preamble.

prosecution altogether. Another difficulty with applying this template is that cybercrime, at its core, is intimately associated with criminal offenses.[75]

In this absence of a defined jurisdiction, "there are no treaties or customary norms that explicitly proscribe the practice" of covert action.[76] While an individual state's internal laws may forbid certain aspects of such actions, there is no international prohibition against states acting as such. Despite the broad definition and existing international law, cybercrime does not allow for an appropriate avenue by which to analyze this note's problem due to the above-mentioned conceptual problems.

B. CYBER-ESPIONAGE

Espionage, in the traditional sense, was the gathering of "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons."[77] Cyber-espionage is merely the newest iteration of states attempting to learn more about their opponents than their opponents can learn about them. As noted above, however, there are no existing international agreements regarding the usage of espionage, cyber or otherwise, by states.[78] Given the lack of an international consensus, international legal scholars have defined cyber-espionage as the use of "a deliberate cyber action that seeks to extract confidential information from . . . [a] computer system or network . . . without the user's knowledge."[79] Alternatively, cyber-espionage has also been similarly defined as "unauthorized probing of a target computer's configuration to evaluate its system defenses or the unauthorized viewing and copying of data files."[80] This definition leaves a great deal of room for interpretation given that "cyber action" is not also explicitly defined, and so could include a wide variety of techniques.[81]

Attempts to use cyber-espionage as a means of analysis are beset by several fundamental problems. First, cyber-espionage concerns

---

[75] Cade, *supra* note 71, at 1144.

[76] Williams, *supra* note 59, at 1165.

[77] A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 600 (2007) (quotation and citation omitted).

[78] Luke Pelican, *Peacetime Cyber-Espionage: A Dangerous but Necessary Game*, 20 COMMLAW CONSPECTUS 363, 370 (2012).

[79] Gervais, *supra* note 12, at 533.

[80] *Id.* at 534.

[81] *See generally id.*

activities that are "used for intelligence and data collection."[82] However, attempting to influence another state's election falls far outside of attempting to "extract the sought-after information"[83] and instead crosses into more affirmative steps. As Weissbrodt describes it:

> The test to determine what constitutes cyber-espionage is simple. If the [state-actor] is only collecting information, then it is cyber-espionage. If the [state-actor] is doing more than merely collecting information, then it is considered to be more than espionage and may rise to the level of use of force or an armed attack.[84]

This relates to another fundamental problem, namely, that cyber-espionage is intended to "obtain information from a computer network without the user's knowledge."[85] However, in order to have an effect on an election, the hacked information must be made public and widely broadcast, which would so put the victims on notice that their computer systems have been compromised. A further difficulty is that cyber-espionage, notwithstanding economic cyber-espionage,[86] is typically conducted by states against other states.[87] As evidenced by the Guccifer 2.0 DNC hacks,[88] though, influential information can be, and is, obtained from private organizations' systems in addition to governmental computer systems. Finally, building off the previous justifications, scholars have argued that cyber-espionage can serve a valuable role in increasing transparency between states.[89] An increase in state transparency is not implicated by attempting to influence another state's elections. For the above reasons, utilizing cyber-espionage as a paradigm of analysis does not allow for an appropriate avenue by which to analyze this note's problem.

---

[82] David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 354 (2013).

[83] Pelican, *supra* note 77, at 365.

[84] Weissbrodt, *supra* note 82, at 372.

[85] Gervais, *supra* note 12, at 533.

[86] *Cf.* Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1167–68 (2014).

[87] *See* Raphael Bitton, *The Legitimacy of Spying Among Nations*, 29 AM. U. INT'L L. REV. 1009, 1010 (2014).

[88] *See generally* Andrew Blake, *Democrats Blame Russia after 'Guccifer 2.0' Hacker Leaks Newest Cache of DNC Documents*, WASH. TIMES (Sept. 14, 2016), http://www.washingtontimes.com/news/2016/sep/14/donna-brazile-russia-guccifer-dnc-hack/; Cory Bennett, *Guccifer 2.0 Drops More DNC Docs*, POLITICO (Sept. 13, 2016, 5:36 PM), http://www.politico.com/story/2016/09/guccifer-2-0-dnc-docs-228091.

[89] Although Bitton discusses this role in terms of traditional espionage, such reasons would seemingly be equally applicable to cyber-espionage. *See* Bitton, *supra* note 87, at 1014.

C. CYBER-ATTACK AND CYBERWARFARE

Cyber-attacks, and the potential for cyberwarfare, also constitute an inadequate means by which to examine the premise of this note. Given the lack of an international agreement regarding states' cyber activities, scholars have defined a cyber-attack as "any action taken to undermine the functions of a computer network for a political or national security purpose."[90] The concept of cyberwarfare also suffers from the problem of "lack[ing a] . . . workable, universally accepted definition[]."[91] Yet, cyberwarfare, as a general concept, "has come to symbolize a state sponsored use of weapons functioning within the cyberspace domain to create problematic and destructive real world effects."[92] These two definitions are related as a matter of degree since an action that begins as a cyber-attack could transition or escalate into cyberwarfare. As such, this note unites these two associated ideas into the same paradigm to allow for ease of analysis, as they can be seen as differing in degree, not in kind.

This paradigm fails to allow for a nuanced analysis of this note's premise due to several problems. First, as noted above, much of the scholarship regarding cyberwarfare is couched in traditional military ideas, principally "[w]hether cyberwarfare constitutes a use of force giving rise to the right of self-defense" under the UN Charter.[93] But "the dominant view . . . has long been that the Article 2(4) prohibition of use of force and the complementary Article 51 right of self-defense appl[ies only] to military attacks or armed violence."[94] As such, whether analyzed under the instrumentality, target, or consequentiality paradigms,[95] a state hacking and releasing information from another state would almost never rise to the level of an armed attack. States subject to such a foreign intervention would therefore have no recourse to any actions under

---

[90] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. R. 817, 826 (2012). The author, however, disagrees with Hathaway et. al's conclusion that any action taken with the intent to disrupt a computer's functioning is a cyber-attack. *Id.* Instead, the author suggests that a more nuanced interpretation would analyze "any cyber action" that aims to undermine or disrupt the function of a computer network as a cyber-attack.

[91] Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N L. JUD. 602, 609 (2011).

[92] *Id.* at 609.

[93] Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. R. 439, 440 (2009).

[94] Waxman, *supra* note 23, at 427.

[95] *See generally* Peagler, *supra* note 17, at 410–11.

Article 2(4), given that such activities do not implicate force.[96] This focus on the use of force also prevents a deeper analysis of underlying issues, such as state sovereignty and the legality of such actions to begin with. Additionally, given the non-physical nature of cyberspace, "attributing a cyber attack to a particular source is one of the most significant challenges"[97] for an examination under the cyber-attack/cyberwarfare paradigm.

D. "CYBER COVERT ACTION"

As can be seen above, cyber law, as it exists today, covers a broad range of activities. However, despite such a broad range, these existing paradigms fail to accurately analyze a state hacking to release information to influence another state's elections. Rather, a new paradigm must be created to allow for any in-depth examination. This note suggests that scholars should transpose previous legal thinking regarding covert actions by states into a new "cyber covert action" archetype. The definition of cyber covert action proposed by this note is based principally upon the US government's definition of covert action.[98] That is to say, a cyber covert action is *any (exclusively) cyber activity or activities of a state undertaken to influence political, economic, or military conditions abroad, where it is intended that the role of the state will not be apparent or acknowledged publicly*. Theoretically, the "an activity or activities" language utilized by the US government[99] could reference cyber actions. Cyber covert action as a new category, however, emphasizes the "cyber" nature of the activity, as opposed to traditional covert action's physical nature.

Utilizing the cyber covert action, as defined above, as a paradigm of analysis allows for a nuanced interpretation of this note's premise. First, covert action "has been a historical mainstay of many states' foreign policies" and so stands on a strong ground of state

---

[96] Conceivably, though, force under Article 2(4) might be implicated if the release of information was part of a nation's cyber-campaign that included more traditional cyber-attacks. In such a situation, the effect of the overall campaign would likely implicate Article 2(4), not just the hacking and release of information. *See* Waxman, *supra* note 23, at 432 (noting that experts believe that "the permissibility and appropriateness of military responses [i.e., force under Article 2(4)] to cyber-attacks should turn at least in part on their effects or consequences").

[97] Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. R. 1079, 1104 (2013).

[98] *See* 50 U.S.C. § 3093(e) (2014).

[99] *Id.*

practice[100] (as opposed to cyberwarfare). Second, utilizing cyber covert action implicates a "sliding scale" of legality, as opposed to a stringent delineation of legal or illegal, under international law.[101] Indeed, under this system, any analysis is tempered by the notion that "the more kinetic or physical the state conduct and the more inconsistent with territorial state laws, the more likely it is to amount to a wrongful exercise of enforcement jurisdiction."[102] Cyber covert action has the distinction of being "a flexible . . . [approach for understanding] operations that lie at the border separating military from intelligence activities,"[103] that is to say, destructive from informational. Finally, unlike other categories of cyber-activities, cyber covert action is not concerned with the intent of the perpetrating actor, but rather with the act itself.[104] This flexibility regarding the intentions and mode inherent in cyber covert action allows for a nuanced discussion of the cyber covert action's legality and impact.

III. INTERNATIONAL LAW AND ITS APPLICABILITY

In Section III, this note will examine the applicability of current international law to the problem of cyber covert actions by countries. This note will examine whether the UN Charter applies to such actions or whether customary international law provides a remedy to impacted states. Finally, the note will examine whether domestic law can apply to cyber covert actions, and whether they provide an appropriate remedy.

A. APPLICABLE INTERNATIONAL LAWS

After being affected by a cyber covert action, which potentially influences a domestic election and incriminates a foreign state, a country might look to international laws and institutions but have little means of recourse. Given its international prominence and extensive membership, the United Nations could be the first place a state might turn to for a resolution. However, under the consequentiality approach,[105] barring a

---

[100] Perina, *supra* note 57, at 520.

[101] Forcese, *supra* note 67, at 81.

[102] *Id.*

[103] Brecher, *supra* note 40, at 434.

[104] *See* Commander Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L.R. 1, 13 (2010).

[105] *See supra* Section I.A.

cyber covert action "with *results* that exceed the Article 51 threshold as an 'armed attack,'"[106] the UN Charter and article 2(4) cannot not directly regulate "nonforcible actions."[107] States subject to a foreign cyber covert action that targets their elections would have no recourse to any action under Article 2(4), given that force is not implicated in a physical sense.[108] Furthermore, "acts of espionage and acts of political . . . coercion within the scope of Article 2(4)" have been purposefully omitted from international law by states,[109] despite the potential for escalation into more traditional "force." As seen here, a state that has suffered from a cyber covert action that targets its elections would have no recourse from the UN Charter, if damage equivalent to an "armed attack" were not also implicated.

Alternatively, a state that has experienced a cyber covert action against itself might attempt to claim a violation of customary international law. Such a claim would likely be a violation of the norm of non-intervention: that the "actions by one state that deny the people of another the opportunity to exercise free political choice violate an international legal obligation."[110] This principle of non-intervention has a clear status under international law, and should be recognized as binding by states.[111] For "[w]hen such [intervening] actions are taken or facilitated by cyber means, they constitute prohibited intervention."[112] As a result, the affected state would, indeed, be correct in claiming such a violation of international customary law.

Such a claim would encounter a significant impediment in that, while a cyber covert action that targets another state's elections would indeed violate customary law, there would be limited options for a remedy. There currently exists no international judicial body whose sole responsibility is to review and adjudicate claims of customary international law. Alternatively, however, a state may be bound by its treaty obligations as "the International Covenant on Civil and Political Rights and regional human rights treaties all embody guarantees of

---

[106] Ryan et al., *supra* note 38, at 1181 (emphasis added); *see* Gervais, *supra* note 12, at 539–41.

[107] Damrosch, *supra* note 10, at 5.

[108] *See generally* TALLIN MANUAL, *supra* note 22, at 45–52.

[109] Beard, *supra* note 70, at 118.

[110] Damrosch, *supra* note 10, at 6.

[111] Lotrionte, *supra* note 45, at 495. *But cf.* Damrosch, *supra* note 10, at 5 ("Because states have tolerated and, indeed, encouraged certain transboundary political activity, international law cannot be said to prohibit all the kinds of external involvement in internal political affairs.").

[112] TALLINN MANUAL, *supra* note 22, at 45.

political participation, with some variations in content."[113] A state may also, by virtue of treaty, end up in front of the International Court of Justice, which is empowered to consider customary international law in its rulings.[114] Whether a state so affected by a cyber covert activity can affirmatively utilize customary international law therefore depends on whether that state has ratified any relevant treaties or both states have consented to granting the International Court of Justice jurisdiction. Another option, discussed below, is for a state to forgo international law and utilize its own domestic laws.

B. DOMESTIC LAWS

Despite the failure of current international law to directly apply to cyber covert actions, a state's domestic laws also fail to offer a perfect remedy. Very briefly, this note will examine whether domestic law can apply to cyber covert action. As noted above, "the more consequential the impact [of the cyber covert action] on the foreign state, the more likely it constitutes intervention violating that state's sovereignty."[115] However, in the United States, only "a small number of existing criminal laws that might govern cyber-attacks explicitly provide for extraterritorial reach."[116] Otherwise, a cyber covert action that affects a state, its territory, or its citizens could likely be considered as conferring jurisdiction to the affected state.[117]

If the state satisfies the jurisdictional requirement, a state so affected would have an excellent claim to being able to impose their domestic law on the perpetrators, regardless of nationality.[118] For example, the United States, under the Computer Fraud and Abuse Act, claims jurisdiction over any hacking that can be used to "to the advantage of any foreign nation."[119] Similarly, in Wisconsin, a foreign state's actor, whose actions impact a computer system in Wisconsin, could likely be prosecuted under either Wis. Stats. §§ 943.70 (2) or (3) for hacking and then releasing information.[120]

---

[113] Damrosch, *supra* note 10, at 38–39.
[114] *See* Forcese, *supra* note 67, at 73–74.
[115] *Id.* at 81.
[116] Hathaway et al., *supra* note 90, at 878.
[117] *See* Raboin, *supra* note 91, at 647–53.
[118] *See id.*
[119] 18 U.S.C. § 1030(a)(1) (1984).
[120] *See* WIS. STAT. §§ 943.70 (2)–(3) (2017).

Domestic law, as a remedy, while likely applicable to the individual actors involved, might still prove to be unsatisfactory. As internationally recognized law professor Ashley Deeks notes, this usage of domestic law may prove to be inadequate for a variety of reasons such as:

> It may be hard for a target state to identify the individuals engaged in the intelligence activity against it, especially when that activity uses complicated, remote technologies. Second, some states may lack a sufficient range of domestic statutes to address these various behaviors, and may have insufficient resources to prosecute such cases when they arise. Third, states may be more tolerant of foreign intelligence activity against disfavored groups (such as minorities) and less willing to pursue domestic remedies on their behalf. Fourth, international law serves an expressive function, and . . . can signal a commitment to providing universal protections against certain troubling acts by states.[121]

Thus, while it may be possible to utilize domestic law to prosecute cyber covert actions, domestic law ultimately represents a stop-gap measure for the failures of international law to comprehensively address either cyber law or covert actions. A more permanent, and effective, solution would be a multi-lateral treaty between states that comprehensively addresses many current issues facing cyber law, particularly those involving cyber covert actions.

IV. A NEW PARADIGM FOR CYBER TREATIES

In Section IV, this note will examine the problem of attribution, which must be noted and accounted for in any effective cyber treaty. This section will then examine Professor Lawrence Muir, Junior's proposed Trilateral Cyber Treaty and explore the intricacies and benefits of such a cyber treaty. This section will conclude by proposing a series of modifications to the cyber treaty to make the proposed cyber treaty more applicable to cyber covert actions.

A. A TRIBUTE TO ATTRIBUTION

Before addressing a possible new paradigm for a cyber treaty, it is important to first address and understand attribution and how

---

[121] Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 613–14 (2016).

attribution can affect any workable cyber treaty. The issue of attribution is one of the trickiest issues surrounding any cyber treaty, and an imperative problem to solve. For attribution is "critical to legitimate claims of self-defense . . . [or] to support reparation claims" by states affected by cyber actions.[122] Attribution, as utilized in this note and scholarly literature, is the "legal and technical . . . identif[ication of] the perpetrator of a cyber attack [or action]."[123] Despite this straightforward definition, conclusively identifying a culprit is anything but straightforward. Attribution is widely considered the "single most difficult element of an offense to prove in a cybercrime."[124]

The underlying cause for difficulties with attribution partially relates to the fundamental design and implementation of the Internet itself.[125] Given the Internet's Cold War origins, "[it] was designed around the core concept of functionality and not based on a design for identification (attribution) and security."[126] As a result, to an extent almost unheard of with physical attacks, cyber-actions can be masked, through such means as proxy servers, virtual private networks ("VPNs"), the TOR software and network, botnets, or other measures that disguise the true origin of a cyber action. Given these techniques for masking an attacker's identity, "[a]ttribution relies heavily on circumstantial evidence, much of which, though scientific, can be called into doubt through the actions" of the perpetrators.[127] Consequently, "it is extremely difficult and sometimes impossible to definitively identify where a cybercrime or cyber-attack originates. And, even if the location is identified, the perpetrator . . . may even remain anonymous."[128]

Given the necessity of positive identification to international law,[129] attribution remains a significant impediment to any workable cyber treaty. Currently, technology does exist, and is being developed to

---

[122] Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C. J. INT'L L. & COMM. REG. 223, 242 (2013).

[123] Major Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167, 172 (2012).

[124] Lawrence L. Muir, Jr., *Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth*, 71 WASH. & LEE L. REV. ONLINE 73, 104 (2014).

[125] Mudrinich, *supra* note 123, at 176.

[126] *Id.*

[127] Muir, *supra* note 124, at 104.

[128] Stephenie Gosnell Handler, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, 48 STAN. J. INT'L L. 209, 213 (2012).

[129] *See generally* TALLIN MANUAL, *supra* note 22, at 29–34.

allow for stronger attribution abilities by governments.[130] Such technology, however, can be utilized by cyber actors to test cyber defenses and does not seem to be widely implemented.[131] As a result, attribution is still hampered by fundamental uncertainty and so must be taken into consideration by any workable cyber treaty.

B. PROPOSED FRAMEWORK FOR A CYBER TREATY

This note suggests that the main manner through which states can address the issue of cyber covert action intended to disrupt elections is through the use of a treaty to prohibit and regulate such conduct. One of the most promising proposed cyber treaties is a trilateral cyber treaty espoused by Professor Muir.[132] This "Cyber Treaty" envisions a treaty between the three main superpowers, namely China, Russia, and the United States.[133] This arrangement is a pragmatic consideration given the current and potential effects of cyber-misfeasance by and affecting each country.[134] This arrangement is also due to the analogous "triangulation" of these same parties during the Cold War, which helped to ease underlying tensions to the benefit of the United States.[135] Underlying this treaty are a series of five guiding goals, the most important of which are to "hold violators of the Cyber Treaty responsible . . . [and to] protect civilian populations."[136]

In order to adhere to these goals, the Cyber Treaty proposes a nomadic neutral tribunal, composed of one judge from each member state.[137] This tribunal would be empowered to adjudicate civil claims relating to violations of the Cyber Treaty's prohibited acts section.[138] The Treaty also attempts to allow states to "identify what assets they seek to protect . . . [and] to circumscribe which acts may be committed by which actors."[139] Once a state brings a matter before the tribunal, the tribunal must decide if the matter in question can be attributed to the responding

---

[130] *Planning for the Future of Cyber Attack Attribution: Hearing Before the Subcommittee on Technology and Innovation Committee on Science and Technology*, 111th Cong. 3 (2010).
[131] *Id.*
[132] *See generally* Muir, *supra* note 124.
[133] *See id.* at 79.
[134] *See id.* at 79–86.
[135] *See id.* at 86–92.
[136] *Id.* at 93.
[137] *See id.* at 94–95.
[138] *See id.* at 95–96.
[139] *Id.* at 101.

state or its actors. To this end, the Cyber Treaty allows for the admission of circumstantial evidence to prove attribution, while still imposing a "clear and convincing evidence" standard.[140] This standard helps to avoid the technical difficulties of attribution,[141] while also allowing the tribunal to make a legally sufficient determination. As can be seen, Professor Muir's proposed treaty creates a workable and efficient, though economically focused,[142] cyber treaty that has real-world implications.

C. ALTERATIONS NECESSARY FOR A WORKABLE CYBER COVERT ACTION TREATY

In many respects, Professor Muir's proposed Cyber Treaty represents an excellent beginning point for a sorely needed and comprehensive cyber treaty. Unlike the Budapest Convention, the Cyber Treaty proposes to affect all currently relevant areas of cyber-activity between countries.[143] The broad nature, and definitions, of this treaty "may be the only realistic option as consensus may only be reached by allowing for differing interpretations."[144] Despite this encompassing nature, cyber covert action, as discussed in this note, still poses uniquely challenging problems that are not directly addressed in the Treaty.[145] Rather than attempt to force cyber covert action into the pre-conceptualized categories of the Cyber Treaty, a more nuanced approach offers several suggested changes to the Cyber Treaty so that it might be more directly applicable to this problem.

One of the principal difficulties of the Cyber Treaty involves the inclusion of Russia as one of the tripartite parties. Rather than a one-time affair, Russia's past and ongoing hacking of both non-governmental and governmental actors in order to influence democratic elections is an ongoing concern.[146] As a result, ratification of the Cyber Treaty would likely flounder or be hampered due to these ongoing political concerns.

---

[140] *Id.* at 104.

[141] *See supra* Section IV.A.

[142] *See* Muir, *supra* note 124, at 103.

[143] *See id.* at 93–94. *But cf.* Budapest Treaty, *supra* note 44, arts. 2–10.

[144] Moore, *supra* note 122, at 242 (citation and quotation marks omitted).

[145] *Cf.* Muir, *supra* note 124.

[146] *See* Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA TODAY (Jan. 9, 2017, 8:01 AM), http://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/; David M. Herszenhorn, *Europe Braces for Russian Hacking in Upcoming Elections*, POLITICO (Dec. 14, 2016, 5:44 AM), http://www.politico.eu/article/europe-russia-hacking-elections/.

Instead, this note suggests that Russia be replaced with the European Union as the third party to the system. This note concedes that doing so would result in losing some, if not many, of the benefits and incentives that Professor Muir proposes.[147] However, such a trade-off would be justified by the comparative benefits of having a (even modified) treaty in place and that such an adjusted Cyber Treaty would be less likely to flounder based upon the political winds blowing against Russia. Furthermore, the adherence by the EU's member-states to such a treaty could help to lead to the development of customary international law regarding cyberspace.

Another important modification to Professor Muir's proposal is adding cyber covert action as a prohibited act to the treaty. Currently, the Cyber Treaty has just three categories of prohibited acts that are to be observed by adhering states: cyberwarfare, cybercrime, and cyber-espionage.[148] Each of these categories touches on some aspect of cyber covert action, whether it be targeting individuals, theft of information, or actions by state-actors. The most topically relevant act, cyber-espionage, is viewed by the Cyber Treaty as having "a similar economic motive to cybercrime, but is tied into the theft of intellectual property."[149] This, in turn, leads to the suggestion that the Cyber Treaty utilize the WTO's dispute settlement process for instances of cyber-espionage.[150] The Cyber Treaty does make a brief note that the treaty "must differentiate between the valid role of cyber-espionage for intelligence agencies—gathering intelligence—and acts that can harm civilians," but does not go into detail as to how the treaty should do so.[151] Therefore, a category of cyber covert action should be added, utilizing Section II.D's definition of that action.[152] This would have the effect of creating a specific category that could be individually enforced, as opposed to trying to adjudicate a cyber covert action under one of the 3 existing categories.[153]

---

[147] *See* Muir, *supra* note 124, at 84–90.

[148] *See id.* at 103–04.

[149] *Id.* at 103.

[150] *See id.* at 93–94. The WTO dispute settlement mechanism is heavily dependent on the institutional bodies, and processes, inherent in the WTO and so would be inappropriate to burden it with a new international legal regime. *See WTO Bodies Involved in the Dispute Settlement Process*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c3s1p1_e.htm (last visited Mar. 19, 2017).

[151] *See* Muir, *supra* note 124, at 103.

[152] *See supra* Section II.D.

[153] *See* Muir, *supra* note 124, at 103–04.

Finally, the Cyber Treaty should provide the tribunal with, in regards to cyber covert action, civil jurisdiction[154] in a manner analogous to the other prohibited acts.[155] Doing so would allow affected member states, in the absence of a criminal court, to obtain some measure of compensation, either for the state or the affected parties.[156] However, as implicitly conceded by Professor Muir, jurisdiction and judgments would rely on the state parties for enforcement.[157] Furthermore, there is a lack of "willingness to enter into multilateral treaties that would allow international tribunals to try their citizens on criminal charges" by the suggested parties.[158] As a result, it would make little sense to attempt to graft criminal jurisdiction regarding cyber covert action onto the tribunal, when the states have indicated little intent to allow such jurisdiction. The limited "extradition forum" envisioned by Professor Muir[159] could be extended to cover cyber covert actions. This would still allow for member states to indict foreign nationals for significant cyber-criminal charges, and "would be an effective first step toward resolving the need to hold people responsible for the damage done by cyberattacks."[160] This forum would be tempered by the requirement that the tribunal determine whether or not the "indictment is supported by probable cause" and if so found, the individual must then be extradited to the indicting country.[161]

Professor Muir's proposed Cyber Treaty is an excellent example of a realistic, and workable, cyber treaty. Rather than a thought exercise, the Cyber Treaty cogently anticipates and addresses real world issues such as state reluctance to provide criminal jurisdiction, the attribution problem, and including a limited extradition forum. Despite the Cyber Treaty's overall strength, the treaty still leaves some room for improvement, notably by the inclusion of an additional cyber covert action category of prohibited acts, the replacement of Russia as a member of the treaty, and extension of the extradition forum to cover cyber covert action.

---

[154] *See id.* at 98–99.
[155] *Id.*
[156] *See id.*
[157] *See id.* at 93–94.
[158] *Id.* at 97.
[159] *Id.* at 97–98.
[160] *Id.* at 97.
[161] *Id.* at 98.

V. CONCLUSION

States originally developed international law in order to craft rules and manage relations between themselves. Since the 1980's, international law has been revolutionized by the "cyber-age." To a certain extent, states have kept pace with these changes by creating "cyber law," which in effect meant updating previous concepts and activities to encompass new "cyber" elements. However, as seen in the 2016 DNC hacks, cyber law is conceptually ill-equipped to handle a state actor hacking and releasing information for the purposes of influencing another country's democratic election process. The currently defined areas of cyber law, such as cybercrime, cyberwarfare, and cyber-espionage, are inadequate for dealing with the complexities of such behavior. Rather, a new conceptual approach should be taken by creating a new category of cyber law, "cyber covert action," in order to adequately describe and analyze such actions. Such a category would encompass the traditional motives of covert action, while also allowing for flexibility in terms of how such activities are carried out in practice.

A state affected by such a campaign would also have little recourse to governing international law, such as the UN Charter and customary international law. Such laws have few effective remedies against such behavior or are otherwise inapplicable due to various definitional requirements. Domestic law, while likely applicable to prosecuting individual actors who engage in such activities, might be a less attractive option for states due to the inherent territorial and jurisdictional requirements.

One solution would be the adoption of a comprehensive multilateral treaty to specifically address the inherent problems identified in cyber and international laws. Professor Muir's Cyber Treaty is an excellent basis for any treaty addressing such problems, and particularly for combatting future attempts at influencing elections through cyber covert action. However, some substantial changes, particularly regarding the tribunal's jurisdictional authority, do need to be made to the Cyber Treaty in order to effectively address cyber covert actions. Cyberspace was once seen as the epitome of democracy; now, unless further action is taken, cyberspace's benefits may prove democracy's undoing.