Loyola of Los Angeles International and Comparative Law Review

Volume 42 | Number 2 Article 3

Spring 2019

# Election Hacking: A Trifecta of Sovereignty, Intervention, and Use of Force Violations in International Law

Arlen Printz

# Election Hacking: A Trifecta of Sovereignty, Intervention, and Use of Force Violations in International Law

ARLEN PRINTZ*

## INTRODUCTION

The 2016 United States Presidential election was riddled with accusations of foreign interference ranging from propaganda, to collusion with candidates, to tampering with the vote-counting systems themselves.[1] While the most serious of these allegations have not been proven, the reality is that the U.S election infrastructure is vulnerable to outside intrusion and even "vote flipping," meaning the altering of individual ballots.[2] These vulnerabilities raise a new problem that must be addressed under international law: if one State hacks into another State's election system and disrupts the infrastructure in such a way as

* Loyola Law School, Los Angeles, Class of 2019. B.A. in History and Minor in Russian 2013, Occidental College. I would like to thank Professor David Glazier for advising me on this Note, as well as the members of the ILR who made this publication possible.

1. *See* Aaron Mak, *Evidence of Russian Election-Data Tampering Mounts as Urgency to Investigate It Does Not*, SLATE (Sept. 1, 2017, 3:10 PM), http://www.slate.com/blogs/the_slatest/2017/09/01/did_russian_hacking_of_vr_systems_affect_election_in_durham_county_new_york.html; *see also* Cynthia McFadden, *William Arkin & Kevin Monahan, Russians Penetrated U.S. Voter Systems, Top U.S. Official Says*, NBC NEWS (Feb. 8, 2018, 7:28 AM), https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721 (describing how Russia gained access to U.S voter rolls in a very select group of states after initially targeting twenty-one of them).

2. *See Election Infrastructure: Vulnerabilities and Solutions*, CTR. FOR AM. PROGRESS (Sept. 11, 2017, 5:43 PM), https://www.americanprogress.org/issues/democracy/reports/2017/09/11/438684/election-infrastructure-vulnerabilities-solutions/ ("42 states use voting machines that are more than a decade old . . . Outdated voting machines pose serious security risks and are susceptible to system crashes, 'vote flipping,' and hacking."); *see also* Tim Starks, *Attack on Commonly Used Voting Machine Could Tip an Election,* Researchers Find, POLITICO (Sept. 27, 2018, 4:08 PM), https://www.politico.com/story/2018/09/27/hacking-voting-machines-814504 (suggesting one model of vote tabulating machine used in 26 states have an "unpatched vulnerability that the manufacturer was notified about a decade ago," and another model used in 18 states that has vulnerabilities that hackers exploited to "gain physical access to a machine… in just two minutes.").

to effectively control the outcome, specifically by altering the ballots themselves and/or their totals, what international law violations do these actions constitute? This note argues that such election hacking constitutes a violation of sovereignty, an unlawful intervention under international law, and should also constitute an unlawful use of force. Only when international law accurately diagnoses the problem can it begin to effectively solve and deter it.

State practice in the cyber context is very new and a lack of State consensus in appropriate responses to various cyber-attacks makes it difficult to determine what, if any, international law violations different cyber-attacks constitute.[3] Without a clear trend of State practice or *opinio juris* relating to cyber-attack classifications and responses, on the surface it seems as if there can be no established customary international law relating to cyber-attacks. But if we analyze the cyber aspect of the attack as a means to an end and instead focus on the nature of the target and the seriousness of the attack's effects, we can more clearly see which areas of international law election hacking violates. While this note only focuses on the most extreme, invasive forms of election hacking, that does not mean that less serious forms of interference cannot themselves be considered a violation of sovereignty, unlawful intervention, or even a use of force. Instead, this note seeks to establish a baseline by classifying the most serious form of election hacking, which for the purposes of this note means altering the vote totals or ballots themselves to control an election's outcome.

The *Tallinn Manual 2.0: On The International Law Applicable To Cyber Warfare* is persuasive authority that currently provides the most widely recognized attempt to establish a framework on how to categorize different cyber-attacks in the context of international law.[4] In 2013 and again in 2017, a group of international law and cyber experts came together on behalf of the Cooperative Cyber Defense Center of Excellence (CCDCOE) to write the Tallinn Manual to advise NATO on international legal issues raised by cyber-warfare.[5] The Tallinn Manual attempts to define existing international cyber obligations as well as

3. JOHANN-CHRISTOPH WOLTAG, CYBER WARFARE: MILITARY CROSS-BORDER COMPUTER NETWORK OPERATIONS UNDER INTERNATIONAL LAW 147 (2014).

4. *See Tallin Manual Process*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, https://ccdcoe.org/tallinn-manual.html (last visited Oct. 27, 2018).

5. Fahmida Rashid, *Security Think Tank Analyzes How International Law Applies to Cyber War*, SECURITY WK. (Sept. 04, 2012), https://www.securityweek.com/security-think-tank-analyzes-how-international-law-applies-cyber-war; *see also* Toomas Hendrick Ilves, *Forward to* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, at xiii (Michael N. Schmitt & Liis Vihul eds., 2d ed. 2017).

encourage the development of new international norms and treaty provisions and apply them to the cyber context.[6] Still, the Tallinn Manual is not a definitive expression or source of law, and its influence on the development of international law remains to be seen.[7] While the Tallinn Manual's framework is sound, its experts overemphasize the importance of kinetic damage over non-physical damage in the application of their "effects" analysis.[8] This emphasis on kinetic damage leads its experts to misapply their framework and incorrectly conclude that election hacking constitutes an unlawful intervention, but not a use of force due to the lack of physical harm.[9]

International law does not necessarily require kinetic damage to occur to classify a State act as a use of force. Article 2(4) of the U.N Charter states that States may not use force against other States' territorial integrity *or* their political independence.[10] Political independence is not a physical concept, and although physical invasions constitute the most obvious threat to a country's independence, so too can non-kinetic assaults on a State's Critical Infrastructure. [11] States designate certain infrastructure as "critical" due to its importance to the individual State,[12] usually for its role in carrying out functions the State deems "essential" or "vital" to its society, such as defense and, as this note will argue, governing elections.[13]

Election hacking, by its nature, raises issues in the well-established and overlapping principles of sovereignty, non-intervention, and the prohibition of the use of force.[14] This note therefore focuses on those three principles as they relate to election hacking and argues that

6. Ilves, *supra* note 5, at xxiv.

7. Johann-Christoph Woltag, *Cyber Warfare,* MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L L., http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e280?prd=EPIL (last updated Aug. 2015).

8. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, 333–334 (Michael N. Schmitt & Liis Vihul eds., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0] (suggesting that *any* cyber-attack that causes physical damage to persons or property will automatically constitute a use of force while non-kinetic attacks that, while they may cause far more damage, must make it through a rigorous multi-part test to constitute a use of force).

9. TALLINN MANUAL 2.0, *supra* note 8, at 313.

10. *Id.*, at 333; U.N. Charter art. 2, ¶ 4.

11. Michael N. Schmitt, *The Use of Cyber Force and International Law*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 1113-14 (Marc Weller ed., 2015).

12. G.A Res. 58/199, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, ¶ 4 (Jan. 30, 2004).

13. Council Directive 2008/114/EC, on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, 2008 O.J. (L 345/75) (EC).

14. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 76 (3rd ed. 2008).

altering the ballots and/or vote totals constitutes a *lex lata* (law as it exists) violation of sovereignty and unlawful intervention. Then, by applying the Tallinn Manual's existing consequence-based analytical framework, this note will make a *lex ferenda* (law as it should be) argument that international law should consider election hacking an unlawful use of force that in some cases rises to the level of an armed attack due to the grave consequences to a victim State's sovereignty and political independence.

Section I provides a historical overview of State interventions organized from least to most invasive and analogizes each to its cyber equivalent, where such an equivalent exists. Even though cyber-attacks are a new phenomenon, State interference in each other's internal processes is not. International law should therefore view cyber-attacks as a new means to familiar ends rather than as an entirely new problem without historical analogy. This note argues that the closest historical equivalent to election hacking is regime change instigated by bloodless foreign backed coups. Both election hacking and bloodless coups can constitute regime change and most significantly, both involve limiting a State's political independence by installing an illegitimate regime of the offending State's choice. While it is true that an offending State may hack in support of the incumbent in the election hacking context, the incumbent would no longer represent the victim State's true choice in leadership. Such a move would be analogous to a foreign-backed coup where a previously democratically elected leader lost an election and, with the help of a foreign government, simply nullified the results instead of stepping down. That leader would no longer be able to claim to represent the sovereign will of the victim State.[15]

Section II defines and explores the related concepts of Critical State Infrastructure and Essential State Functions. This section argues that election infrastructure constitutes both Critical Infrastructure as well as an Essential State Function. The Critical Infrastructure designation is an important gauge of what States view as essential functions, which is highly relevant in determining whether a specific

15. *See* Georg Nolte, *Intervention by Invitation*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L L., http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1702?prd=EPIL (last updated Jan. 2010) (describing how Afghanistan's leader invited the Soviets to intervene in an internal conflict on his behalf, but was himself overthrown and killed two days into the intervention, raising doubts about the legitimacy of the initial invitation); *see also* G.A. Res. ES-6/2 (Jan. 14, 1980) (describing the Soviet intervention as an "Armed Intervention" and a sovereignty violation, heavily implying that it did not recognize the invitation presented by the new puppet government to the Soviets as a legitimate expression of Afghanistan's sovereign will).

attack constitutes a violation of sovereignty, an unlawful intervention, an unlawful use of force, or all three.

Section III is divided into two parts. Section A argues that election hacking constitutes a violation of sovereignty according to the 1928 Island of Palmas Arbitration's articulation of sovereignty.[16] Section B argues that election hacking constitutes a prohibited intervention in line with the I.C.J decision, Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (hereinafter Nicaragua Judgment). This case dealt with the United States' active support of armed rebel groups, the Contras, against the Nicaraguan government during the 1980s, and provides an authoritative and uncontroversial statement on what constitutes a prohibited intervention according to customary international law.[17]

Section IV takes a consequences-based approach to determine whether election hacking rises to the level of a use of force. This means it gives heavy weight to the actual effects of the attack, rather than making the existence of a kinetic equivalent of the cyber-action determinative in deciding whether it constitutes a use of force, an armed attack, or neither.[18] This section will make use of the Tallinn Manual's proposed factors to determine if an action rises to the level of a use of force. These factors include the severity of the consequences (the most important factor), the immediacy of the consequences, the directness between the attack and the consequences of the attack, the invasiveness of the attack, the measurability of the attack's effects, the military character of the attack, State involvement in the attack (for the purposes of this note, State involvement will be assumed), and finally, the presumptive legality of the action.[19] This section applies these factors and the reasoning in the Nicaragua Judgment to foreign backed coups and election hacking in order to ensure conformity with existing expressions of customary international law.[20]

Section V analyzes whether election hacking rises to the level of an armed attack. The analysis is almost identical to the use of force analysis with the added factor of intent, borrowed from the Case Concerning Oil Platforms (Iran v. U.S.) Judgment.[21] This section

16. Agreement Concerning Island of Palmas, Neth.-U.S., Jan. 23, 1925, 2 R.I.A.A. 829.

17. GRAY, *supra* note 14, at 75.

18. YAROSLAV RADZIWILL, CYBER-ATTACKS AND THE EXPLOITABLE IMPERFECTIONS OF INTERNATIONAL LAW 138 (2014).

19. TALLINN MANUAL 2.0, *supra* note 5, at 333-336.

20. *See* GRAY, *supra* note 14, at 75.

21. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. Rep. 161, ¶¶ 51, 64, 67, 89, (Nov. 6) [hereinafter Oil Platforms, Judgment].

acknowledges that not all uses of force will rise to the level of an armed attack. This distinction is important because an armed attack may trigger a State's inherent right of self-defense, which is in essence a lawful use of force to stop an attack, while a lesser use of force will not.[22] Using the severity analysis from Section IV, Section V will argue that international law should recognize the possibility that election hacking may rise to rise to the level of an armed attack. This note does not seek to give States an excuse to inflict violence on each other. It only seeks for international law to recognize the seriousness of election hacking so that the international community may more effectively cooperate to deter such behavior.

## I. A BRIEF HISTORY OF INTERVENTIONS AND THEIR EQUIVALENTS IN CYBER-SPACE

States have interfered in each other's internal affairs, including elections, long before the advent of cyber-space. Professor Calder Walton, an Ernest May Fellow at the Kennedy School of Government who specializes in espionage research, classifies such interventions as "active measures."[23] These measures range from mere propaganda campaigns intended to influence a foreign State's public opinion, intervening in elections themselves by funding preferred candidates, to covert acts of force aimed at regime change.[24]

At the less invasive end of the active-measures spectrum lie propaganda campaigns. Walton describes how, during the 1984 United States presidential election, the Soviet Union detested President Ronald Reagan[25] and spread propaganda via an infiltration campaign of the Democratic National Committee to suggest that Reagan's election would mean war.[26] While the technology changed, analogous interventions took place in 2017, when Russia, the Soviet Union's successor State, was accused by Spanish officials of using online social media to "heavily promote Catalonia's independence referendum…in

22. Karl Zemanek, *Armed Attack*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L L., ¶¶ 4, 8, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e24 (last updated Oct. 2013).

23. Calder Walton, *"Active Measures:" A History of Russian Interference in US Elections*, PROSPECT MAG. (Dec. 23, 2016), http://www.prospectmagazine.co.uk/science-and-technology/active-measures-a-history-of-russian-interference-in-us-elections.

24. *Id*.

25. *Id*.

26. *Id*.

an attempt to destabilize Spain."[27] Spain claimed that it detected a number of fake accounts on social media, half of which it traced back to Russia.[28] This type of interference was similar to Russia's alleged efforts to sow division and undermine other elections, most notably in the United States election of 2016.[29]

More invasive than spreading propaganda, States have taken more aggressive steps in interfering in each other's elections by directly supporting their preferred candidates. The United States, for example, intervened in the Italian election of 1948. Not only did the United States spread damaging misinformation about Socialist candidates in a propaganda campaign, but it also used the CIA to funnel money to support moderate candidates to ensure a reliably anti-Communist Italian government came to power.[30] The United States' direct monetary support of preferred Italian candidates constituted a more severe intervention and a higher degree of control over the outcome than a simple misinformation campaign.

Even more serious interventions can be found in the modern cyber context. Russia, for instance, allegedly launched a three-pronged cyber-attack on Ukraine in its 2014 election.[31] Russia first allegedly used a friendly hacker group, CyberBerkut, to "shut down Ukraine's Central Election Commission's computer systems by disrupting the internal network."[32] While the Ukrainian government was able to get the system back online in time for the election, Russia also allegedly attempted to falsify vote totals of the preliminary results, which would have declared ultra-nationalist Dmytro Yarosh the winner, when, in reality, he received less than one percent of the vote.[33] The Ukrainian government caught the change before publicly releasing the preliminary results.[34] Finally, Russia allegedly launched Distributed Denial of Service Attacks against Ukraine's voter tallying system, which effectively

27. *Spain Sees Russian Interference in Catalonia Separatist Vote*, REUTERS, (Nov. 13, 2017, 8:23 AM), https://www.reuters.com/article/us-spain-politics-catalonia-russia/spain-sees-russian-interference-in-catalonia-separatist-vote-idUSKBN1DD20Y.

28. *Id*.

29. Mak, *see supra* note 1.

30. *See* Walton, *supra* note 23.

31. Jason Le Miere, *Russia Election Hacking: Countries Where the Kremlin Has Allegedly Sought to Sway Votes*, NEWSWEEK (May 9, 2017, 5:55 PM), http://www.newsweek.com/russia-election-hacking-france-us-606314.

32. Gabe Joselow, *Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past*, NBC NEWS (Nov. 3, 2016, 2:18 AM), https://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246.

33. Le Miere, *supra* note 31.

34. Joselow, *supra* note 32.

blocked election results for two hours, though the final results were deemed a "genuine election" by international observers.[35]

These alleged attacks against Ukraine's elections by Russia were particularly egregious, and were likely part of its overall campaign to undermine Ukraine, which included even more serious actions like Russia's 2014 annexation of Crimea.[36] It is, however, important to note that Russia did not alter the actual ballots or the *final* vote totals, and thus did not alter the ultimate outcome of the election.[37] While effective and incredibly invasive, these efforts still allow the victim State a measure of choice. Because Russia left the *final* vote totals alone, it can be inferred that the intent behind the hack was not to instigate regime change, but rather to undermine trust in the Ukrainian election process. Similarly, and to a far lesser extent, the CIA certainly influenced the 1948 Italian election, but it did not completely usurp the Italian State's election process as its people were still free to accept or reject the CIA's misinformation and elect a candidate of their choice. While one can argue the choice was corrupted by the offending State, the choice in leadership was ultimately still the victim State's own. These interventions therefore do not rise to the most serious type of active measures: regime change.

One infamous example of foreign-instigated regime change was the 1953 coup in Iran. Sixty-four years later, the CIA admitted to, and released details pertaining to, its involvement in the 1953 Coup that removed Iranian Nationalist leader Mohammad Mossadegh.[38] In 1953, the CIA colluded with a number of high ranking conspirators in the Iranian army and government in an effort to remove Mossadegh for nationalizing Iran's oil industry.[39] Ironically, the coup almost failed soon after it began.[40] Mossadegh had somehow caught wind and almost foiled the coup.[41] The coup only succeeded when Kermit Roosevelt Jr.,

35. Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' From Hackers*, CHRISTIAN SCI. MONITOR (June 7, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

36. Daniel Treisman, *Why Putin Took Crimea: The Gambler in the Kremlin*, FOREIGN AFF. (Apr. 18, 2014), https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea.

37. Joselow, *supra* note 32.

38. Bethany Allen-Ebrahimian, *64 Years Later, CIA Finally Releases Details of Iranian Coup*, FOREIGN POL'Y (June 20, 2017, 1:43 PM), http://foreignpolicy.com/2017/06/20/64-years-later-cia-finally-releases-details-of-iranian-coup-iran-tehran-oil/.

39. *Id*.

40. *Id*.

41. *History of Iran: A Short Account of 1953 Coup Operation Code-name: TP-AJAX,* IRAN CHAMBER SOC'Y (Nov. 21, 2017), http://www.iranchamber.com/history/coup53/coup53p2.php.

the CIA's head operative in Iran, ignored an order from his superiors to abandon the mission.[42]

After discovering the plot, Mossadegh dissolved the Iranian parliament in an effort to consolidate power, but this only aided the American effort by making him appear authoritarian.[43] Roosevelt and General Zahedi, a high-ranking Iranian conspirator who had gone into hiding, figured that the coup could succeed so long as they convinced the population that the Shah had signed two decrees: one removing Mossadegh from office and a second making Zahedi the "lawful" Prime Minister.[44] After much intrigue, the CIA helped smuggle key coup plotters into the embassy compound to prepare for the coup once the prime minister's guard was down.[45] While the CIA ultimately lost control of the situation, pro-Shah crowds began to gather, the Shah's decrees were finally published in Iranian newspapers, and Roosevelt helped General Zahedi out of hiding and get to a radio station where he spoke to the nation as the "rightful" prime minister and cemented the new regime's power.[46]

The 1953 coup is a prime example of regime change carried out by one State's agents against another State without resorting to a full-scale invasion. By forcibly replacing Mossadegh with a leader of their choice, the United States and its allies effectively deprived the Iranian State of its political independence. This subtler and (relatively) bloodless form of regime change is an appropriate analogy for international law when considering the implications of election hacking. If, for instance, Russian efforts in Ukraine had not stopped at changing the preliminary results but had also altered the ballots or the *final* results to suggest their chosen candidate won, Russia would have gone beyond sabotage and completely usurped Ukraine's internal process of choosing its leaders and thus its political independence.

While it is true that a military coup uses force in the conventional, physical sense and election hacking does not, both utilize Critical Infrastructure within the victim State to achieve the same result: a traditional coup will utilize the victim State's existing military infrastructure to install an illegitimate government of the offending State's choice, while an election hack will utilize the victim State's election infrastructure to achieve the same result. Both types of regime

42. Allen-Ebrahimian, *supra* note 38.
43. *See History of Iran*, *supra* note 41.
44. *Id*.
45. *Id*.
46. *Id.*

change are achieved by attacking and using a victim State's Critical Infrastructure against it.

## II. THE IMPORTANCE OF STATES' CRITICAL INFRASTRUCTURE

There is currently no universally accepted list of what can constitute "Critical Infrastructure," though the counter-terrorism arm of the U.N. recognizes that Critical Infrastructure encompasses cyber infrastructures.[47] Aside from this acknowledgment and the recognition of Critical Infrastructure's importance, the U.N has not defined it, instead "recognizing that each State determines what constitutes its critical infrastructure."[48] Despite the lack of a definition, the existence of, and need for, protection of Critical Infrastructures within States is still a widely accepted idea in the international community and supported by a number of treaties and U.N resolutions.

In 2004, the United Nations General Assembly adopted a resolution entitled, the "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures," which urges member States to protect their Critical Information Infrastructures, a subset of Critical Infrastructure, to achieve cyber-security.[49] The resolution goes on to encourage member States to share their "best practices" with the rest of the international community to ensure better international cyber-security.[50] Finally, the resolution encourages member States to trace breaches to their infrastructure and report the source of the attacks, specifically, in order to prevent and respond to them.[51] The existence of this resolution indicates that States take intrusions into their Critical Infrastructures very seriously, which not only implies a general obligation under customary international law not to interfere in or otherwise sabotage other States' Critical Infrastructure, but also implies that such an attack is much more likely to be considered an unlawful intervention, if not a use of force. Despite recognizing the concept of Critical Infrastructures, the fact that the resolution leaves its

47. U.N. Office of Counter-Terrorism, Protection of Critical Infrastructure Including Vulnerable Targets, Internet, and Tourism Security, https://www.un.org/counterterrorism/ctitf/en/protection-critical-infrastructure-including-vulnerable-targets-internet-and-tourism-security (last visited Oct. 14, 2018).

48. S.C. Res. 2341 (Feb. 13, 2017).

49. *See generally* G.A. Res. 58/199, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, (Dec. 23, 2003).

50. *Id*. at 2.

51. *Id*. at Annex: ¶¶ 4, 7, 9.

definition up to individual States makes it difficult to determine a clear, customary international law definition.[52]

The practice of leaving the definition of Critical Infrastructure up to member States can also be found in a 2004 agreement between the United States and Canada to protect the border and their respective "Critical Infrastructure."[53] Similar to the General Assembly Resolution, this treaty defines Critical Infrastructure as, "Governmental and/or private activities or sectors that are identified by each party in its laws, executive orders, or policies as 'Critical Infrastructure.'"[54] We must therefore turn to Canadian and United States domestic law respectively. Canada has a broad approach, defining its Critical Infrastructure as, "processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, or economic well-being of Canadians and the *effective functioning of government*" (emphasis added), which can easily be read to include Election Infrastructure.[55] The United States, by contrast, more narrowly defines Critical Infrastructure as "certain national infrastructures [that] are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[56]

Initially, the United States specifically included "telecommunications, electrical power systems, gas and oil, storage and transportation, banking and finance, transportation, water supply systems, emergency services…and [a vague] continuity of government" in its list of what constitutes Critical Infrastructure.[57] Only as recently as January 6, 2017 did the United States Department of Homeland Security designate its elections systems as Critical Infrastructure under the "Government facilities" sector, which also includes national monuments and icons, and education facilities.[58] In defining "election infrastructure," then-head of the Department of Homeland Security, Jeh

52. *Id*. at 1.

53. Agreement Between the Government of Canada and the Government of the United States of America for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security, Can.-U.S., Dec. 12, 2001, T.I.A.S. No. 04-601, art. I [hereinafter U.S.-Can. Agreement].

54. *Id*.

55. PUB. SAFETY CAN., NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE, 2 (2009) (emphasis added), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

56. Exec. Order No. 13,010, Critical Infrastructure Protection, 61 Fed. Reg. 37, 347 (July 15, 1996).

57. *Id*.

58. U.S. ELECTION ASSISTANCE COMM'N, STARTING POINT: U.S. ELECTION SYSTEMS AS CRITICAL INFRASTRUCTURE, 1-2 (2017), https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

Johnson, enumerated storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.[59]

Given the discretionary nature of Critical Infrastructure, some scholars are wary about using it as a basis to determine violations of international law, especially in terms of an unlawful use of force, as States may abuse the Critical Infrastructure concept by interpreting it too widely to justify an otherwise unjustifiable use of force as self-defense.[60] While this fear is understandable, the classification of election infrastructure as Critical Infrastructure in international law is warranted, as will be explored below.

The European Union maintains a 2008 treaty, with similar provisions to the 2000 U.S.-Canada Treaty, which seeks to identify and protect its member States' Critical Infrastructure.[61] The European Union defined Critical Infrastructure as an,

> [A]sset, system, or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.[62]

The European Union's definition, while more restrictive than previous iterations which leave the "Critical Infrastructure" entirely up to the States, is more in line with existing international law notions of sovereignty, non-intervention, and human rights. For instance, the International Covenant on Civil and Political Rights (ICCPR) adopted by the U.N General Assembly states,

> Every citizen shall have the right and opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions: (a) To take part in the conduct of public affairs, directly or through freely chosen

59. Press Release, Secretary Jeh Johnson, Dep't of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical#wcm-survey-target-id.

60. RADZIWILL, *supra* note 18, at 138.

61. Council Directive 2008/114/EC, *supra* note 13, at art. 1.

62. *Id*. at art. 2, § (a).

> representatives; (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors.[63]

It is important to note that not every "vital" societal interest will constitute an "essential state function" under international law. To constitute an "essential state function," the function must govern a matter that international law gives States exclusive control over.[64] Following the European Union's understanding of Critical Infrastructure, and applying it to the ICCPR, States' election systems are not only vital to societies that have elections, but also they are "essential" to those States' internal decision-making processes and their governments' legitimacy in the eyes of the local population, international human rights law, and traditional principles of State sovereignty. As the mechanism that facilitates the voting requirements of the ICCPR and through that, State decision-making, election systems embody a nexus between popular and State sovereignty. Election systems therefore constitute both Critical Infrastructure *and* the essential State function of choosing its own leaders. An attack on election infrastructure, cyber or otherwise, therefore constitutes an attack on a State's Critical Infrastructure *and* essential State function, which in turn invokes the overlapping international law concepts of sovereignty, unlawful interventions, and use of force.

## III. SOVEREIGNTY AND UNLAWFUL INTERVENTIONS IN THE ELECTION HACKING CONTEXT

### *A. Sovereignty in Essential State Functions*

The first question is what exactly states have sovereignty over. The 1928 Island of Palmas Arbitral Award, a case involving a territorial dispute between the Netherlands and United States, articulates a widely accepted definition of Sovereignty:

> Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other

63. International Covenant on Civil and Political Rights, pt. III, art. 25, Dec. 19, 1966, 999 U.N.T.S. 171.

64. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 205 (June 27) [hereinafter Military and Paramilitary Activities, Judgment]; *see also* Agreement Concerning Island of Palmas, *supra* note 16, at 838.

> State, the functions of a State . . . Territorial sovereignty. . . involves the exclusive right to display the activities of a State.[65]

On the surface, the territorial definition of sovereignty poses a unique problem in the cyber context since cyber-space is not a physical space. But cyber-space cannot exist, at least currently, without physical manifestations that anchor it to the physical world. Moreover, these physical manifestations, such as servers, data centers, and undersea cables that connect cyber processes, are analogous to "key terrain" targeted in conflict like the high ground in land battles and sea lines in naval ones.[66] The Tallinn Manual came to the conclusion that States exercise sovereignty over not only the physical manifestation of cyber infrastructure, but *also* the "logical and social layers" of their infrastructure, with "the physical layer consisting of the physical network components, the logical layer consisting of the connections that exist between network devices, and the social layer consisting of individuals engaging in cyber activities."[67] This is not just a recommendation, however, and according to international cyber law expert, Yaroslav Radziwill, many States currently do claim sovereignty over "their" cyberspace, especially when the physical infrastructures that support it are located within their territory.[68]

While sovereignty over the physical manifestations of cyber infrastructure is not disputed when such infrastructure lies within the physical territory of a State, the question still exists as to whether States maintain sovereignty over "their" cyber-space that is not represented by physical components located entirely or mostly within the State's territory.[69] Still, election infrastructure is State Critical Infrastructure governing an essential State function over which the State has a right to maintain exclusive control. Therefore, a fair reading of the Island of Palmas decision echoed in the Nicaragua Judgment extends beyond territorial sovereignty and gives States sovereignty over all their essential functions. States have a right to decide freely the

65. Agreement Concerning Island of Palmas, *supra* note 16, at 838-39.

66. John R. Mills, *The Key Terrain of Cyber*, GEO. J. INT'L. AFF. (SPECIAL ISSUE) 2012, at 99-100 (crediting Prussian military theorist Carl von Clausewitz (1780-1831) with coming up with the principles of "key terrain, which refers to "vital ground" that must be gained to get the upper hand on an opponent).

67. TALLINN MANUAL 2.0, *supra* note 5, at 12.

68. RADZIWILL, *supra* note 18, at 107.

69. *See* Kurt Mackie, *Microsoft Dublin Datacenter Case Getting Supreme Court Review*, REDMOND MAG. (Oct. 16, 2017), https://redmondmag.com/articles/2017/10/16/microsoft-dublin-datacenter-case.aspx (explaining how the U.S government tried to force Microsoft to turn over data stored overseas, but Microsoft refused. This raises issues of sovereignty over data beyond the scope of this note that have not yet been resolved).

implementation of all their essential functions, regardless of the (lawful) method or location they choose to execute them in.[70] This means that State A would maintain sovereignty over its essential functions even when those functions are carried out within a consenting State B's infrastructure.

The second question with regard to sovereignty is its violation. According to the Tallinn Manual, "Cyber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law."[71] The Tallinn Manual's suggested rule in regard to cyber-space is consistent with the sovereignty rights outlined in the Island of Palmas decision and Nicaragua Judgment. Because States maintain exclusive rights over their essential State functions, meddling with those functions does not require kinetic damage to find a breach of sovereignty. What matters, especially in the cyber context, is if one State has inserted itself into an essential State function of another State without that State's consent.

By breaking into a State's election system physically or via a cyber-attack and altering the vote count, a State will violate the victim State's sovereignty because it will have usurped the essential State function of vote counting. A State's election infrastructure and vote counting process goes to the heart of its leadership selection process and therefore its political independence. Whether the new leader chosen by the offending State actively serves the offending State or not, or indeed whether the offending State's chosen candidate "wins" their election at all, does not matter for the purpose of finding a violation of sovereignty. By breaking into and attempting to usurp the essential State functions of vote counting and choosing its leaders, the offending State has violated the sovereignty of the victim State if one reads customary international law as recognizing State sovereignty over their essential State functions. Not only does such election hacking constitute a breach of the victim State's sovereignty, it constitutes an unlawful intervention as well.

### *B. Coups and Election Hacking: The Ultimate Unlawful Intervention*

Closely intertwined with the concept of sovereignty is the principle of unlawful intervention. The prohibitions of unlawful intervention and unlawful use of force are customary international laws, and the Nicaragua Judgment provides an authoritative statement on the law in

70. Military and Paramilitary Activities, Judgment, *supra* note 64, ¶ 205.
71. TALLINN MANUAL 2.0, *supra* note 5, at 17.

this area.[72] For an intervention to be considered "unlawful," according to the Nicaragua Judgment,

> The principle [of non-intervention] forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, *by the principle of State sovereignty* (italics added), 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 regards to such choices, which must remain free ones.[73]

To summarize, to be considered an unlawful intervention, an action taken against a State by one or more other States must contain two elements. First, the action must be carried out by a State or agents the State retains effective control over, who then interfere in matters which are "solely the responsibility of the inner State actors," such as an essential State function.[74] Second, the action must contain an element of coercion. Coercion means the application of various kinds of pressure including but not limited to threats, intimidation, and the use of force to compel one State to think or act in a certain way.[75]

In addition to the Nicaragua Judgment's statement on customary international law, the U.N Charter provides its own prohibition on both force and interventions more generally when it states, "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, or *in any other manner inconsistent with the purposes of the United Nations* (emphasis added)."[76] It is that latter clause, "in any other manner inconsistent with the purposes of the United Nations," which is most relevant to the non-intervention principle.[77]

The General Assembly clarified the non-intervention principle in its Declaration on Principles of International Law Concerning Friendly

---

72. GRAY, *supra* note 14, at 75.

73. Military and Paramilitary Activities, Judgment, *supra* note 64, ¶ 205.

74. Philip Kunig, *Intervention, Prohibition of*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. ¶ 1, http://etron.lls.edu:2177/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?rskey=TqufOg&result=1&prd=EPIL (last updated Apr. 2008).

75. Christopher Joyner, *Coercion*, MAX PLANCK ENCYCLOPEDIA PUBLIC INTERNATIONAL LAW ¶ 1, http://etron.lls.edu:2177/view/10.1093/law:epil/9780199231690/law-9780199231690-e1749?rskey=jxgt4o&result=1&prd=EPIL (last updated Dec. 2006).

76. U.N. Charter art. 2, ¶ 4.

77. *Id*.

Relations and Co-operation Among States in Accordance with the Charter of the United Nations. The declaration states,

> The General Assembly … convinced that the strict observance by States of the obligation not to intervene in the affairs of any other State is an essential condition to ensure that nations live together in peace with one another, since the practice of any form of intervention not only violates the spirit and letter of the Charter, but also leads to the creation of situations which threaten international peace and security… solemnly proclaims the following principles ….[78]

The resolution goes on to state that, "States shall conduct their international relations in the economic, social, cultural, technical and trade fields in accordance with the principles of sovereign equality and non-intervention,"[79] which includes "the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter."[80] Given the U.N. charter wording and General Assembly clarifications, the customary international law principle of non-intervention is a cornerstone of U.N. principles, and military force is *not* a prerequisite for violating the law of non-intervention.

On the surface, the element of coercion may seem to require some kind of threat and demand made by the offending State of the victim State for an unlawful intervention to exist under international law. However, the key phrase in the I.C.J. decision is "choices which *must* (emphasis added) remain free ones."[81] One reason the United States ran afoul of the non-intervention principle in the Nicaragua Judgment was because the United States provided weapons and logistical support to armed bands actively trying to overthrow the Sandinista government;[82] thus threatening the State's choice in political systems, and as a result, its political independence. Or to put it another way, the actions of the United States were coercive because they tried to compel the Nicaraguan State to change to a regime more favorable to the United States. Both election hacking and coups are analogous to this kind of coercion directed at the heart of State Sovereignty: its choice in leadership.

78. G.A. Res. 25/2625, annex, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, at 2 (Oct. 24, 1970).

79. *Id*. at 6.

80. *Id.* at 3.

81. Military and Paramilitary Activities, Judgment, *supra* note 64, ¶ 205.

82. *Id*. ¶ 241.

While the Nicaragua facts largely concern uses of force, the ruling's wording, when considered alongside the Declaration on Principles of International Law Concerning Friendly Relations, suggests that *any* action that usurps or attacks an essential State function or a State's political independence will likely constitute a violation of the norm of non-intervention, regardless of the presence of military force. While it is true that some interventions, such as spreading propaganda, are so minor they likely lack the coercive element necessary to be considered unlawful interventions, election hacking and coups invariably have that coercive element by usurping choice entirely in a way that mere propaganda does not.

In the case of a foreign-backed coup, the offending State takes control over elements within the victim State's military infrastructure to forcibly install a regime of the offending State's choice, thus usurping the results of the victim State's essential internal function of choosing its leaders. In the case of election hacking, the Tallinn Manual unequivocally declares ballot tampering via cyber-attacks an "illegal intervention."[83] This conclusion is consistent with the elements outlined in the Nicaragua Judgment. Because the requirement is coercion, the question is whether election hacking constitutes an attempt by one State to compel another State to act in a certain way. In the election-hacking context, by hacking into State B's election infrastructure which has been shown to be Critical Infrastructure regulating the essential State Function of vote counting, State A is effectively using its cyber power to usurp State B's sovereign right to elect the leader of its choice. According to the Declaration of Friendly Relations among States, choosing one's own leadership must remain a free choice.[84] By hacking into and altering State B's election outcome, State A has hijacked Critical Infrastructure within State B and used it to usurp an essential State function that goes to the heart of State B's political independence. It has therefore unlawfully interfered in a choice that must remain free by coercing the victim State into choosing a leader against its will.

## IV. ELECTION HACKING AS A USE OF FORCE

Article 2(4) of the U.N. charter, which respected commentators such as Christine Gray regard as a codification of customary international law,[85] reads, "All Members shall refrain in their international relations from the threat or use of force against the

83. TALLINN MANUAL 2.0, *supra* note 5, at 313.
84. G.A. Res. 25/2625, *supra* note 78, at 5.
85. GRAY, *supra* note 14, at 76.

territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[86] As in the case of unlawful intervention, the charter largely leaves the term "use of force" up to interpretation with concern for territorial integrity and political independence of member States at the forefront. The Tallinn Manual experts extrapolate that a "[c]yber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[87] This standard is problematic in that it fails to account for the possibility that as the world increasingly relies on the Internet, a destructive cyber-attack may not have a non-cyber equivalent. This standard is better seen as temporary until cyber-norms have a chance to develop into customary international law of their own, but for now, it serves as a useful bridge to connect existing international law governing physical attacks to their cyber equivalent. Drawing this link is especially useful in the use of force context to persuade commentators unwilling to characterize an action as a use of force unless they can analogize it to well-established forms of force, hence the analogy of election hacking to a foreign-backed coup.

The scope of the prohibition of the use of force is subject to much debate even in the physical realm, and the line between an unlawful intervention and an unlawful intervention that constitutes a use of force is a fuzzy one.[88] The most widely accepted definition among commentators on the prohibition against the use of force comes from the Nicaragua Judgment.[89] There, the court makes clear how the prohibition against force significantly overlaps with the prohibition against unlawful intervention; immediately following its discussion of prohibited interventions, the opinion states,

> The element of coercion, which defines and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, whether in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State. General Assembly resolution 2625 (XXV) equates assistance of this kind with the use of force by the assisting state when the acts committed in another state involve a threat or use of force. These forms of actions are therefore wrongful in the

86. U.N. Charter art. 2, ¶ 4.
87. TALLINN MANUAL 2.0, *supra* note 5, at 330.
88. GRAY, *supra* note 14, at 30.
89. *Id*. at 75.

> light of both the principle of the non-use of force and that of non-intervention.[90]

The United States had funded the Contra rebels against the Sandinista government of Nicaragua and also supplied them with weapons and logistical support.[91] While the funding alone only constituted a violation of the principle of non-intervention and violation of sovereignty,[92] directly attacking oil platforms, placing mines at Nicaraguan ports, and arming the rebels constituted a breach of Nicaragua's sovereignty, a violation of the norm of non-intervention, *and* a prohibited use of force.[93] Supplying an armed group with weapons was a trifecta of unlawful use of force, unlawful intervention, and violation of sovereignty, while supplying an armed group with money was only an unlawful intervention and violation of sovereignty.[94] Still, the court did not establish that the kind of force leveled against Nicaragua was the minimum threshold of what constitutes a use of force against a State. The court did lay out a "scale and effects" test related to the use of force, but this test was to determine whether an already established use of force was tantamount to an armed attack, which, unlike a lesser use of force, could trigger the victim State's right of self-defense against the aggressor State.[95] Without a similar test for what constitutes a use of force to begin with, scholars have been left to debate the minimum threshold.

This note takes a "contextualist" approach in its use of force analysis, which contends that coercion is a common element of unlawful interventions and unlawful uses of force, and that interventions fall along a continuum ranging from relatively non-invasive interventions that lack a coercive element like propaganda, to unlawful interventions like funding a rebel army, and prohibited uses of force and armed attacks.[96] The contextualist approach is also effects-centric and holds that international law should classify actions by the harm to the victims and the aims of international law as represented by

---

90. Military and Paramilitary Activities, Judgment*, supra* note 64, ¶ 205.
91. *Id.* ¶ 241.
92. *Id.* ¶¶ 228, 251.
93. *Id.* ¶ 251.
94. *Id.* ¶¶ 228, 251.
95. *Id.* ¶ 195; *see also* Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. Rep. 161, ¶¶ 51, 64 (Nov. 6) [hereinafter Oil Platforms, Judgment] (following the *Nicaragua* court's reasoning in distinguishing armed attacks from lesser uses of force to hold that Iran's attack on the ship, *Sea Isle City*, did not constitute an armed attack and, therefore, did not trigger a right of self-defense from the U.S.).
96. *See generally* Heather Harrison Dinniss, Cyber Warfare and the Laws of War 62-63 (2006).

the U.N. charter without requiring that harm to be physical in nature.[97] This school is represented by scholars such as Michael Schmitt, who is best known for his work in the realm of international cyber-law.[98]

The contextualist approach is especially helpful in the cyber realm since cyber-attacks can result in non-kinetic, but still catastrophic damage to a State's interests as well as to the U.N. charter's goals of peace, stability, and respecting the political independence of its member States.[99] Because of its flexibility, the Tallinn Manual embraces this contextualist approach in a multi-factor "scale and effects" test derived from the Nicaragua Judgment and Schmitt's writings to determine when a cyber-attack rises to the level of a use of force.[100] Because the Nicaragua Judgment draws a distinction between a use of force and an armed attack by using a scale and effects test to determine the line between them, it is logical to apply a similar scale and effects test to determine the line between a coercive act that constitutes an unlawful intervention and one that constitutes an unlawful use of force. The Tallinn Manual framework is extremely useful in the election hacking context. This note will therefore apply the Tallinn Manual factors as far as they align with the Nicaragua Judgment's reasoning to determine if election hacking constitutes a use of force.

To define the "scale and effects" test laid out in the Nicaragua Judgment, the Tallinn Manual adopts a test analyzing eight factors to determine if a particular action rises to the level of a use of force including severity, immediacy of the consequences, directness between the attack and its consequences, invasiveness of the action, measurability of the attack's effects, military character of the attack, state involvement, and presumptive legality of the action.[101] All "reasonably foreseeable consequences" of the cyber-attack may be considered for the use of force analysis.[102] For example, if State A arms a rebel group in State B, a reasonably foreseeable consequence is the use of those weapons against State B's government. Thus, that effect may be considered in determining whether arming the rebel group

97. *Id.*; *see also* Nicholas Tsagourias, *Cyber Attacks, Self-Defense, and the Problem of Attribution*, 17 J. Conflict & Security L. 229, 231 (2012) (claiming that any attack on a "critical state infrastructure that paralyses or massively disrupts the apparatus of the State should be equated to an armed attack, even if it does not cause any immediate human injury or material damage." The commentator cites an attack on a State's financial system that "causes massive disruption to the economic life of a State" as an example.).

98. *See* Schmitt, *supra* note 11.

99. *See* U.N. Charter art. 1, ¶ 2, art. 2, ¶¶ 1-4.

100. Tallinn Manual 2.0, *supra* note 5, at 331.

101. *Id*. at 334-36.

102. *Id*. at 343.

constitutes a use of force. Similarly, if State A alters the ballots and / or vote count for State B's election, an illegitimate government coming to power in State B is a reasonably foreseeable consequence and may be considered in the use of force factors test.

### *A. Severity*

The severity of the attack, which is the most important and determinative factor, analyzes the scale of harm to the victim State, subject to a *de minimis* test where physical harm to individuals or property will always qualify as a use of force regardless of the intent behind the action, while attacks generating mere "inconvenience or irritation" will not.[103] Arming rebels as in the Nicaragua case would meet this test, assuming the weapons were used and hit their targets, and would likely cross this threshold even if the rebels ousted the government with the threat of force alone as in a bloodless coup. By contrast, propaganda that simply irritates the victim state and inconveniences it by introducing a harmful narrative to combat but otherwise causes no damage will never constitute a use of force. But when harm is not physical and there is no obvious threat of physical force, this factor will look at the "critical national interests" affected and the scope, duration, and intensity of the attack's consequences.[104]

The nature of the target is critical here, and an attack on critical State Infrastructure should be considered strongly indicative of meeting the dispositive severity factor. A minority of the Tallinn Manual's experts who back this view argue that an attack on a State's Critical Infrastructure should be considered an armed attack if the consequences, kinetic or otherwise, are severe enough.[105] For the purposes of this analysis, a Critical Infrastructure designation is strongly indicative of a State's "Critical National Interest," since the designation requires States to view the infrastructure as important enough to their national interest to label them "Critical" in the first place.[106]

Election infrastructure is a vehicle for the internal decision-making process that must remain exclusive to the State, as per the customary international law definition of sovereignty outlined in the Island of Palmas decision.[107] It is the assault on this process rather than physical damage to the voting machines that cause the most damage to a State;

103. *Id.* at 136, 334.
104. *Id*. at 334.
105. *Id*. at 343, 345.
106. Exec. Order No. 13,010, 61 Fed. Reg. at 37347.
107. Agreement Concerning Island of Palmas, *supra* note 16, at 838.

machines can be repaired, but if the process itself is attacked by altering vote counts, even if the attack is discovered and corrected, a major consequence will be a loss of faith by the victim State's populace in its election infrastructure. This loss of confidence is especially significant in democratic forms of government which derive their legitimacy from their people's faith that the process accurately reflects the popular will.[108] The consequences of a successful hack are even more severe.

Election infrastructure represents the essential State function of choosing its own leaders, which is central to a State's political independence and also its sovereignty.[109] A significant and especially severe consequence of election hacking is the usurping of an essential State function in choosing its leaders if the hacking is not detected in time. Even if the election hacking aided the incumbent rather than the opposition party, a successful, uncorrected attack still usurps the internal decision-making process of the State and through that its political independence, as the incumbent no longer reflects the popular will reflected by the State's unaltered internal process.

The ultimate goal and, arguably, the most severe consequence of actions such as election hacking, orchestrating a coup, and supporting armed rebel groups is to usurp a State's political independence. The Tallinn Manual recognizes the severity of targeting and removing a State's leadership when it declared that a cyber-attack that kills a head of State abroad is tantamount to not just a use of force but an armed attack as well.[110] The fact that election hacking achieves this goal without physical violence does not minimize the threat or damage to a State's political independence by the rightful leader's removal nor does it matter if the offending State does not control the usurpers once they take power.[111] Indeed, the effects of election hacking on a victim State's political independence have the potential to be even more severe than those of an assassination since election hacking not only removes a rightful leader from power, but also decides the successor. Because of the nature of the attack, the nature of the targets (in this case an attack on a State's Critical Infrastructure that usurps an essential State function), and the severity of the consequences of assaulting a State's

108. W. Michael Reisman, *Sovereignty and Human Rights in Contemporary International Law*, 84 AM. J. INT'L L. 866, 868-69 (1990).

109. Agreement Concerning Island of Palmas, *supra* note 16, at 838.

110. TALLINN MANUAL 2.0, *supra* note 5, at 346.

111. *See* Military and Paramilitary Activities, Judgment, *supra* note 64, ¶ 115 (explaining that the Nicaragua Court established an "effective control" test in order to find one State responsible for the paramilitary group's actions. However, this standard is used to establish State responsibility, *not* severity).

very political independence, customary international law's prohibition of the use of force should at a minimum be read to include election hacking.

### *B. Immediacy of the Consequences*

The second factor that the Tallinn Manual describes is the immediacy of the consequences. This factor reasons that the quicker the consequences of an attack manifest themselves, the less time States have to peacefully resolve the dispute or otherwise mitigate the harmful effects. Therefore, States will be more likely to treat attacks with immediate consequences as a use of force compared to attacks where the consequences have a slow-drip effect that builds over time.[112] In the case of election hacking, this factor may lean against finding a use of force since there could be months in between the revealing of the false vote totals and the new illegitimate leader ascending to office. On the other hand, the transition of power would potentially begin immediately after the election is called.[113] Still, this factor is less critical to the analysis than the severity factor, as evidenced by the Nicaragua court finding that arming rebels can constitute an unlawful use of force.[114] The actual effects of that support may not have been felt for months after the fact, but that did not at all mitigate finding an unlawful use of force in the court's reasoning.[115] Far more important is where the consequences lie in the chain of causation described below.

### *C. Directness of the Consequences*

The third factor considers the directness between the attack and its consequences. Essentially, an attack where the direct consequences are slight, but lead to greater indirect harm in the chain of causation, are less likely to be deemed a use of force by States than attacks that cause direct harm.[116] Applying this reasoning to the Nicaragua Judgment, the direct consequence of the United States arming the Contras was armed attacks carried out by the Contras, while the direct consequence of simply funding the Contras was one step removed: they had to purchase

112. TALLINN MANUAL 2.0, *supra* note 5, at 334.

113. *See* Julie Hirschfeld Davis, *Trump's Transition in a 'Long History' of Rocky Presidential Handovers*, N.Y. TIMES (Nov. 16, 2016), https://www.nytimes.com/2016/11/17/us/politics/obama-white-house-transition.html (describing how the transfer of power in the United States normally begins within days after the election).

114. Military and Paramilitary Activities, Judgment*, supra* note 64, ¶ 95.

115. *Id*. ¶¶ 195, 237.

116. TALLINN MANUAL 2.0, *supra* note 5, at 334.

their own armaments before they could carry out armed attacks. Even though the reasonably foreseeable consequences of funding the Contras were the Contras arming themselves and carrying out attacks with those armaments, the court reasoned that directly arming them constituted a use of force, while merely providing funding did not.[117] Following this reasoning, the direct consequences of election hacking are the changing of the ballots and the installing of an illegitimate government; there is no intermediary step. Unlike the case of arming rebels or organizing a coup, where action by the rebels or coup plotters is required before the harm occurs, there is no intermediary independent action required by the State precisely because the ballots themselves represent the State's independent decision. By altering them, the offending State has effectively removed that independent choice from the victim State, making the consequences of election hacking extremely close to the attack in the chain of causation. The directness factor between the attack and the harm therefore leans in favor of a use of force.

### *D. Invasiveness of the action*

The fourth factor is invasiveness. This factor analyzes how secure the hacked system is, with more secure systems indicating a greater degree of importance to the victim State: the more secure the system, the more likely its hacking will be viewed as a use of force.[118] Additionally, the Tallinn Manual experts fold in an 'intent' analysis where the more the effects of an attack are limited to the targeted state, the more invasive the attack will be perceived.[119] However, the Tallinn Manual experts make clear that mere espionage will never be enough to constitute a use of force on its own, regardless of how invasive the operation, unless the espionage damages the networks in the process.[120] Still, the effectiveness of a country's security measures, or lack thereof, do not necessarily indicate the importance of the infrastructure being hacked, and the Tallinn Manual experts merely provided one method of determining the importance of different cyber infrastructures to a State. The invasiveness factor should therefore not depend on the difficulty of the hack alone. Rather, the invasiveness analysis should focus on the nature of the target and how closely it is tied to essential State functions, the State's sovereignty, and if it qualifies as Critical Infrastructure.

117. Military and Paramilitary Activities, Judgment*, supra* note 64, ¶¶ 109, 118.
118. TALLINN MANUAL 2.0, *supra* note 5, at 334.
119. *Id*. at 335.
120. *Id*.

In the case of election hacking, the invasiveness analysis is very similar to the severity analysis given election systems' likely status as Critical Infrastructure and their central role in a State's decision-making process that goes to the heart of its political independence. Additionally, the effects of election hacking are very deliberate and very limited to whichever State systems were hacked. Thus, the invasiveness analysis heavily leans in favor of finding a use of force.

### *E. Measurability of Effects*

The fifth factor is the measurability of effects. This factor reasons that the more apparent and quantifiable the consequences of the operation are, the more likely a State will be willing to characterize an action as a use of force.[121] Applying this factor to the Nicaragua Judgment's reasoning, there was a measurable number of arms supplied to the Contras, and their use resulted in measurable harm. This factor essentially requires an attack to have an objective measure of damage to lean in favor of a use of force. In the case of election hacking, there are measurable effects: the number of ballots altered, or the difference between the manufactured results and the real results, are easily measurable numbers. In the coup context, somewhat ironically, the "objective and measurable" criteria are lacking in that the only "measurable harm" will be the damage and collateral damage involved in removing the old regime, which may very well be minimal if the coup is efficient enough. In the case of coups, as in the case of election hacking, what is ultimately threatened are the political independence and sovereignty of States, which are not easily quantifiable principles. However, their respect lies at the heart of customary international law as well as the U.N. Charter.[122] It would therefore be highly illogical to consider an assault on them less likely to constitute a use of force simply because the offending State figured out a way to usurp a victim State's political independence without inflicting easily quantifiable harm. Thus, even if the effects of an attack are largely subjective, they, as in the case of attacks that usurp a country's political independence and sovereignty, can still be extremely severe. The severity factor is therefore, ultimately, the most important factor and significantly outweighs the measurability of effects in the eight-part test.

121. *Id*. at 335-336.
122. U.N. Charter art. 1, ¶ 2, art. 2, ¶¶ 1–4.

### *F. Military Character of the Attack*

The sixth factor is the military character of the attack. This factor is a holdover from the traditional view of the use of force, and thus makes a "military character" attack more likely to be considered a use of force than an attack without "military character."[123] The Tallinn Manual justifies the inclusion of this factor by citing the U.N. Charter's preamble, which reads, "We the Peoples of the United Nations determined to save succeeding generations from the scourge of war. . .And for these ends. . .to ensure. . .that armed force shall not be used, save in the common interest."[124] "Military Character" therefore implies a type of armed force employed by State militaries against a victim State's military targets.[125] The Nicaragua court made particular issue of the type of aid provided by the United States to the Contras, and application of this factor to the court's reasoning helps to explain why supplying rebel soldiers with weapons to fight a State's government, a clearly militaristic action, is more likely to constitute a use of force than simply providing that same rebel group with funds that can be used for a variety of purposes.[126] A foreign backed coup may invoke this "military character" factor by utilizing the offending State's intelligence apparatus to control elements within the victim State's military to achieve forcible regime change, as demonstrated by the U.S.-backed coup in Iran.[127] Similarly, the scale of a successful election hacking operation may utilize an offending State's military infrastructure in carrying out cyber-attacks, which would give the attack a military character.[128] But, election hacking may also lack this military character as an offending State may be able to utilize lone hackers unaffiliated with its military. In addition, the targeted election systems, while Critical Infrastructure, are not understood to have a military character.[129]

123. TALLINN MANUAL 2.0, *supra* note 5, at 336 (citing to the DOD MANUAL: OFFICE OF THE GENERAL COUNSEL U.S. DEPARTMENT OF DEFENSE (June 2015), para.16.3.1: "Cyber operations that cripple a military's logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force under jus ad bellum").

124. U.N. Charter, Preamble.

125. TALLINN MANUAL 2.0, *supra* note 5, at 336.

126. Military and Paramilitary Activities, Judgment*, supra* note 64, ¶ 228.

127. *History of Iran*, *supra* note 41.

128. *See China Military Unit 'Beyond Prolific Hacking'*, BBC NEWS (Feb. 19, 2013), https://www.bbc.com/news/world-asia-china-21502088 (discussing the rumors of how a cyber-unit of the Chinese military is responsible for stealing "hundreds of terabytes of data from at least 141 organizations all around the world." If the hackers are indeed associated with the Chinese military, this attack could be said to have a "military character" under the Tallinn Manual's parameters).

129. U.S. Election Assistance Commission, *supra* note 58, at 1.

Still, because of election Infrastructure's deep ties to a State's sovereignty and political independence, the severity factor should significantly outweigh the possible lack of military character in the election hacking context.

### *G. State Involvement*

The seventh factor is State involvement and, through that, State responsibility. This factor asserts that the clearer the "nexus" between the attack and its official agencies, the more likely a victim State will consider the attack a use of force.[130] For the purposes of this note, it is assumed that the offending State maintains "effective control" over the agents responsible for hacking into State B's election systems.[131] By extension, State responsibility is pre-assumed for the purposes of the election hacking analysis.

### *H. Presumptive Legality*

The eighth and last factor is presumptive legality. This factor reasons that because "international law is generally prohibitive in nature, acts that are not forbidden are permitted."[132] If an action is not considered a different violation of international law under existing rules, a State is less likely to consider the action an unlawful use of force. A relevant example here is the spreading of propaganda to influence a State's populace: the action is not considered an unlawful intervention or even a violation of sovereignty and, thus would be highly unlikely to constitute a use of force.[133] By contrast, every time the court in the Nicaragua Judgment found an action to constitute an unlawful use of force, it had also found that same action to constitute another international law violation, usually a violation of sovereignty and/or unlawful intervention.[134] This is not to say that an additional international law violation is a *prerequisite* to the existence of an unlawful use of force but merely that if one action violates international law for a different reason, it increases the chance the illegal action will constitute a use of force as well. And, if the action is not presumably illegal, it is less likely to be seen as an unlawful use of force.

---

130. TALLINN MANUAL 2.0, *supra* note 5, at 336.

131. *See* Military and Paramilitary Activities, Judgment, *supra* note 64, ¶ 115 (describing how a State must have "effective control" over a group in order to be held legally responsible for the actions of said group).

132. TALLINN MANUAL 2.0, *supra* note 5, at 336.

133. *Id*.

134. Military and Paramilitary Activities, Judgment, *supra* note 64, ¶¶ 228, 241, 251.

Because election hacking is already presumed illegal, in that it violates State sovereignty and constitutes an unlawful intervention, and because the measurability of the effects factor, invasiveness factor, directness factor, and all-important severity factor all heavily lean in treating election hacking as a use of force, international law should recognize election hacking as an unlawful use of force as well.

## V. ELECTION HACKING AS AN ARMED ATTACK

As a general rule, an armed attack will always constitute a use of force, but a use of force may not always rise to the level of an armed attack.[135] This distinction between a use of force and armed attack matters because an armed attack can trigger a State's right to individual and collective self-defense, while a use of force below that threshold does not.[136] All the factors that were analyzed in the use of force section, including reasonably foreseeable consequences, directness, and severity, also apply to determining whether the action rises to the level of an armed attack. But, because self-defense, to be lawful, must be both proportional and necessary to repel the armed attack suffered,[137] victim States must also consider the intent of the offending State as well as whether the action is sufficiently grave to justify an armed response. Intent and meeting the graveness threshold are not factors; they are necessary elements in finding an armed attack.

### *A. Intent*

The court in Oil Platforms (Iran v. U.S.), a case that involved the attack on a U.S. ship with Iranian sea mines, implied that a lack of intent will mitigate against finding that an individual use of force constitutes an armed attack.[138] If an attack was accidental, future attacks are unlikely to follow, so any force used in response to the accidental attack would be a retaliation rather than an act of self-defense. Conversely, as in the case of a coup or election hacking, regime change constitutes the explicit intent behind both operations. Therefore, the "intent" element should be satisfied in both election hacking as well as a

135. Oil Platforms, Judgment, *supra* note 21, at 187, 191.

136. *Id.*; *see also* U.N. Charter art. 51, ¶ 1 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* (italics added) occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.").

137. Christopher Greenwood, *Self-Defence*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e401?prd=EPIL (last updated Apr. 2011).

138. Oil Platforms, Judgment, *supra* note 21, ¶¶ 51, 64.

foreign-backed coup. But intent alone is not dispositive of an armed attack; it is merely a necessary element.

### *B. The Graveness Threshold*

The current customary international law as described in the Nicaragua Judgment is vague in describing when a use of force rises to the level of an armed attack, saying only that its scale and effects must be sufficiently "grave."[139] In the cyber context, experts are divided on the type of approach to use, with some advocating a "strict liability" approach which would treat any attack on a State's Critical Infrastructure as an armed attack, and others advocating an effects-based approach, which looks at the scope and severity of the attack's effects.[140] The strict liability approach, while tempting in its simplicity, suffers due to a lack of consensus regarding what constitutes "Critical Infrastructure" in the first place as well as the fact that the effects on said Critical Infrastructure may be minor.[141] The effects-based approach, on the other hand, more closely resembles the Nicaragua Judgment's focus on the actual consequences of the attack and thus is the approach this note embraces.[142] Therefore, consideration of the nature of the target, e.g. election infrastructure that has been demonstrated to constitute Critical Infrastructure, will be folded into the severity analysis which will determine if an action is sufficiently "grave" to constitute an armed attack.

### *C. The Consequences to Consider*

As in the use of force analysis, the Tallinn Manual's experts unanimously agreed that only "reasonably foreseeable consequences" should be considered in determining if a use of force constitutes an armed attack.[143] For instance, if an attack targets a water purification plant, the damage to the plant will, in and of itself, constitute a use of force, but the resulting sicknesses from tainted water should also be taken into account when deciding if that use of force rises to the level of an armed attack because sickness from tainted water is a reasonably foreseeable consequence of an attack on a water purification center.[144] Similarly, in the coup and election hacking contexts, regime change and

139. Military and Paramilitary Activities, Judgment*, supra* note 64, ¶¶ 191, 195.
140. RADZIWILL, *supra* note 18, at 138.
141. *Id*.
142. *Id*.
143. TALLINN MANUAL 2.0, *supra* note 5, at 343.
144. *Id.*

a limiting of the victim State's political independence are reasonably foreseeable consequences of that kind of attack.

### *D. Directness*

The armed attack analysis, to be consistent with the Nicaragua Judgment, must weigh the "directness" factor more stringently than in the use of force analysis.[145] Even though the United States clearly intended the weapons it supplied to the Contras to be used in armed attacks against the Nicaraguan government and that their use was a highly foreseeable consequence, the court was *not* willing to classify arming rebel group as an armed attack.[146] The act of supplying the weapons was one step removed from their use in the chain of causation that caused the damage. In order to hold the United States responsible for the armed attacks carried out with the supplied weapons, Nicaragua needed to demonstrate that the United States maintained "effective control" over the Contras' actions and that the Contras were "subject to the United States to such an extent that any acts they have committed are imputable to that State," which it had failed to do.[147] The foreign-backed coup context may suffer from a similar directness problem since the offending State will invariably work with internal actors within the victim State, similar to the United States working with the Contras in Nicaragua. Merely providing these actors with the means to achieve regime change, given the Nicaragua standard, will not be enough to classify this use of force as an armed attack. The victim State would have to demonstrate that the offending State had "effective control" over the coup plotters.[148] Election hacking, by contrast, does not trigger the directness problem.

As explained in the use of force analysis, an election hack does not suffer from an indirectness classification precisely because there is no friendly agent required in the victim State. If a State provided actors within another State with the means to hack into their own election systems and instructed them in how to achieve this, that would be analogous to arming a rebel army, and the Nicaraguan court's "effective control" standard would have to be demonstrated before ruling the incident an armed attack. However, with a direct hack, there is no friendly intermediary required within the victim State; there is only the direct attack into a State's Critical Infrastructure. This means that the

145. Military and Paramilitary Activities, Judgment*, supra* note 64, ¶ 195.
146. *Id*.
147. *Id*. ¶¶ 115-16.
148. *Id*.

more stringent directness factor does not weigh against treating direct election hacking as an armed attack. With the more stringent directness factor and intent factor weighing in favor of an armed attack, the only factor left to consider is severity.

### *E. Severity*

The severity analysis in the armed attack context is similar to the use of force analysis. The Advisory Council on International Affairs took the position, since adopted by the Netherlands, that a cyber-attack *must* be regarded as an 'armed attack' within the meaning of Article 51 of the U.N. Charter if it causes (or has the potential to cause) serious disruption to the functioning of the [S]tate or serious or prolonged consequences for the stability of the [S]tate, even if there is no physical damage or injury, with a *de minimis* recommendation against counting a mere "impediment" or "delay" of State functions.[149] So, while a cyber-attack that merely slows down the voting machines or otherwise confuses the voters may not pass the *de minimis* threshold, altering the election results almost certainly does. First, election hacking attacks the State's Critical Infrastructure itself. Second, as in the case of a coup, election hacking usurps the essential State function of choosing its own leaders. Finally, it installs an illegitimate government against the victim State's wishes, which, in turn, usurps the victim State's political independence.

It must be acknowledged that the Nicaragua Judgment was unwilling to find the existence of an "armed attack" that did not involve some sort of physical damage or "armed bands . . . on a significant scale."[150] At first glance, it may seem like hackers constitute a loophole to this "armed bands" standard. However, many States incorporate cyber-activities into their militaries and intelligence agencies. Russia, for instance, maintains a dedicated unit of "internet trolls" that wages propaganda campaigns against its perceived enemies.[151] China maintains a figurative army of hackers that launch ninety thousand attacks a year against U.S. Defense Department computers.[152] A hacker force armed with cyber-weapons descending upon a State's Critical infrastructure

149. Advisory Council on International Affairs, *Cyber Warfare*, No. 77, AIV/No. 22, CAVV 36 (Dec. 2011).

150. Military and Paramilitary Activities, Judgment*, supra* note 64, ¶ 195.

151. Maya Kosoff, *The Russian Troll Farm that Weaponized Facebook had American Boots on the Groun*d, VANITY FAIR (Oct. 18, 2017, 9:44 AM), https://www.vanityfair.com/news/2017/10/the-russian-troll-farm-that-weaponized-facebook-had-american-boots-on-the-ground.

152. Gerald Posner, *China's Secret Cyberterrorism*, THE DAILY BEAST (Jan. 12, 2010, 8:02 PM), https://www.thedailybeast.com/chinas-secret-cyberterrorism.

should logically meet this "armed band" standard. The avenue of attack should not matter. What matter are the scale and effects of the attack.

## CONCLUSION

Many international law commentators are resistant to classifying attacks that do not result in death or physical destruction as a use of force or armed attack. Though the Tallinn Manual experts more readily accept that non-kinetic attacks can constitute a use of force, some of its experts still take the position that a non-kinetic use of force can *never* rise to the level of an armed attack.[153] However, the purpose at the heart of self-defense—prohibitions on the use of force, unlawful interventions, and violations of State sovereignty—is to protect the political independence and "sovereign equality" of States.[154] Surely, an attack that threatens every one of these principles at once must qualify as among the gravest uses of force. The classification of election hacking as a violation of sovereignty, unlawful intervention, *and* use of force that may rise to the level of an armed attack is not a call to arms. It is a call to reality in recognizing the severity of usurping a State's political independence.

153. TALLINN MANUAL 2.0, *supra* note 5, at 342.
154. U.N. Charter art. 2, ¶ 1.