Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage

A clear principle has not yet developed in international law to deal with State-conducted cyber activities that cause harm to other states but do not directly cause physical damage. One method of conducting such a cyber activity is to carry out a “distributed denial of service” (DDoS) attack. DDoS attacks prohibit a user from accessing a digital resource by bombarding the network with digital requests to use the resource. The principle of non-intervention provides one avenue for applying current international law to DDoS attacks that are not immediately physically destructive. Under the principle of non-intervention, such attacks would be internationally unlawful if they amounted to coercion of the target state. This application would be consistent with past applications of non-intervention and would provide a more helpful framework for analyzing the international legality of non-destructive DDoS attacks than other areas of customary law or the Charter of the United Nations.
INTRODUCTION

Many Americans might never have heard of the film THE INTERVIEW\(^1\) were it not for the international controversy surrounding it. Following the release of the 2014 film, premised on a United States plot to assassinate North Korean leader Kim Jong Un using two incompetent reporters—played by Seth Rogen and James Franco—Sony Pictures’ internal email system was hacked, resulting in the destruction of data and the leak of a large volume of Sony’s internal emails to the public.\(^2\) The United States quickly blamed North Korea, whose government was reportedly insulted by the subject of the comedy.\(^3\) Soon after Sony’s information was leaked, North Korean computers across the country lost access to the internet. Although the United States did not claim official responsibility, North Korean authorities asserted their belief that the U.S. was responsible.\(^4\)

Although a number of inferences must be drawn in order to fill in the relevant actors and actions in this sequence of events, the scenario provides an ideal example of twenty-first century statecraft. Gone are the days when the phrase “armed attack”\(^5\) was sufficient to delineate unacceptable behavior between states. When applying customary international law to new circumstances international courts and scholars typically try to analogize the new circumstances to past circumstances that have been explicitly addressed by international

---

1. THE INTERVIEW (Columbia Pictures 2014).
With the advent of new “cyberwarfare” techniques that are not always readily analogous to traditional techniques that are the subject of customary international law, there is a substantial gray area when determining acceptable state-to-state online behavior.

The politics and moral questions of the fifteenth century world of early international legal scholars like Grotius and Suarez were in many ways just as complex as those of the twenty-first century world of Rogen and Franco, but the methods of inflicting harm upon other states were relatively straightforward. These methods included plundering foreign vessels and towns, attacking and killing citizens using military force, starving populations using blockades, dethroning foreign monarchs, conquering foreign territory, and capturing foreign citizens to sell into slavery. Discerning the actor and the harm resulting from each of these methods was not usually a difficult task.

Today, states can disrupt and destroy resources and technology in other states using operatives whose reach extends from a suburban office building to anywhere in the world. These attacks can range from temporarily limiting access to a single webpage to shutting down a nuclear reactor. Determining international legal obligations applicable to cyber activities presents a significant challenge to international law.

Scholars typically focus on forms of cyber intrusion with the potential to cause physical damage in a state. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence convened a group of international experts in Tallinn, Estonia to compile an authoritative interpretation of existing international law’s application to cyberwarfare, the Tallinn Manual. The experts were able to conclude that cyber attacks causing physical damage or harm are violations of the prohibition on the threat or use of force embodied in the Charter of the United Nations (U.N. Charter). However, scholarship in inter-

---

6. See Rosalyn Higgins, Problems and Processes: International Law and How We Use It 10 (1994) (discussing the ability to reason by analogy in applying existing international law to apparent “lacunae” in modern law).


8. For a comprehensive appraisal of international law and cyberwarfare, including the predominant views of a number of global scholars on the topic, see Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael Schmitt, ed. 2013) [hereinafter Tallinn Manual] (setting out ninety-five “black letter” rules governing international cyber conflict, as agreed by a panel of 20 international law experts).


10. This development is heavily influenced by Michael Schmitt’s scholarship. See Mi-
national law has not specifically addressed the issue of whether there is a legal prohibition on Distributed Denial of Service (DDoS) attacks that do not result in physical damage comparable to the damage inflicted by traditional “kinetic” force, such as destruction of property or harm to individuals. I refer to these as “non-destructive DDoS attacks.”

In late 2016, the second Tallinn Manual (Tallinn 2.0) will be released. This manual attempts to perform the same function as the first manual, but for international law of cyber-space beyond the humanitarian regime. The first Tallinn Manual discussed only international cyberlaw surrounding uses of force, but the group of experts also indicated a willingness to accept that cyber attacks below the force threshold could violate non-intervention. This may indicate that Tallinn 2.0 will contain a detailed discussion of cyber interventions.

In this Note, I argue that DDoS attacks that cause no physical damage are violations of the principle of non-intervention if they deprive the target state of sufficient control over critical infrastructure so as to constitute coercion. In Part II, I discuss the international legal background of the concepts of the prohibition on the use of force, the principle of non-intervention, and the use of non-destructive DDoS attacks. In Part III, I address the challenges of applying the prohibition on the use of force to non-destructive DDoS attacks because of (1) the difficulty of identifying the perpetrators and (2) the lack of international legal support for applying the prohibition on the use of force to attacks that are not physically destructive. I also identify the challenges in applying the principle of non-intervention. In Part IV, I explain the benefits of addressing non-destructive DDoS attacks through the lens of the customary law of non-intervention, including the applicability of the standard of coercion to such attacks. My approach addresses non-destructive DDoS attacks as violations of the principle of non-intervention that do not involve the use of force.


BACKGROUND

Prohibition on the Use of Force in International Law

One of the most fundamental values of the international system is respect for the sovereign equality of states. This is the first principle articulated in Article 2 of the U.N. Charter. The sovereign equality of states affirms a state’s right to make its own decisions about its political system, laws, foreign policy, and most other functions within its own territory. The only limits on the sovereign power of each state are the rights of other states, and the human rights of each state’s people.

The most prominent corollary of the international principle of sovereign equality is the prohibition on the threat or use of force. This prohibition is codified in Article 2(4) of the U.N. Charter, and states that 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.” The U.N. Charter commits states to peaceful settlement of disputes. The prohibition articulated in the U.N. Charter is an attempt to codify a customary norm prohibiting the use of force. Scholars disagree about whether the customary norm is identical to the norm expressed in Article 2(4). Commentary typically focuses on the language in Article 2(4) of the “territorial integrity or political independence of any state” to determine whether the customary norm of non-use of force prohibits more activity than the U.N. Charter’s articulation. Thus, Article 2(4) of the U.N. Charter has legal weight either as a treaty obligation to its 193 signatories or as an independent customary rule.

17. Id., at art. 2, ¶ 2.
Principle of Non-Intervention

The principle of non-intervention is closely related to the use of force. It arises out of the same principle of sovereign equality.21 In its earliest formulation, the principle was only understood to prohibit influencing another state by using force. This formulation is frequently attributed to Emer de Vattel, who, without employing the language of “interference” or “intervention,” argued that European intervention in New World states using force violated the laws of war.22 This definition continued to inform discussions of non-intervention into the twentieth century, as scholars interpreted the principle to prohibit “dictatorial” interference with another state.23

The International Court of Justice expounded on the principle in its judgment in the Case Concerning Paramilitary Activities in Nicaragua. The court articulated a clearer definition of the activity prohibited and the types of matters that could be subject to unlawful intervention. The court stated that the principle was part of customary international law. This prohibited states from interfering in affairs of other states when the matter being interfered with was one whereby the target state was “permitted, by the principle of State sovereignty, to decide freely.”24 It included in this category “. . .choice of a political, economic, social, and cultural system, and the formulation of foreign policy.”25

Along with the characteristic that an unlawful intervention bears on a matter the state is entitled to decide freely, the court noted that a violation of non-intervention required coercion:

. . .intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. 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, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed

25. Id.
activities within another state.\textsuperscript{26}

The concept of “coercion” in international law closely follows, but does not mirror, its common usage. Coercion occurs when an actor attempts to persuade another actor to take a certain course using force or presenting negative consequences for taking an alternative course.\textsuperscript{27} In international law, coercion does not include only actions taken for the purpose of influencing another state to change policy. It also includes more direct forms of interference such as attempting to recognize a secessionist movement that has not yet achieved statehood.\textsuperscript{28} Such interference directly deprives the target state of control over its borders, rather than influencing it to act in a certain way by causing or threatening harm.

Despite the court’s opinion in \textit{Nicaragua}, the exact scope of behavior prohibited by non-intervention is hard to define. This is due to the vague language codifying the norm in various multilateral agreements and resolutions, as well as the puzzling practice of states claiming to adhere to non-intervention.\textsuperscript{29} This confusion led one twentieth century scholar to remark that “[t]he only interesting question regarding the principle of non-intervention in international law is why on earth anyone should assume that it exists.”\textsuperscript{30} Nevertheless, modern scholars generally agree that non-intervention is part of customary international law though broad disagreement exists about its scope.\textsuperscript{31}

The principle is frequently discussed in U.N. General Assembly Resolutions. As stated in the 1970 Declaration on Friendly Relations, a 1970 General Assembly Resolution purporting to codify customary international law: “No State or group of States has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other State.”\textsuperscript{32} The Declaration fur-

\textsuperscript{26.} Id.
\textsuperscript{29.} See Lori F. Damrosch, \textit{Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs}, 83 Am. J. Int'l L. 1 (1989) (arguing that although the international community widely agrees that the principle of non-intervention is part of customary law, state practice is insufficient to support a broad view of this norm).
\textsuperscript{32.} G.A. Res. 2625 (XXV), annex, Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the
ther explains the principle to prohibit “economic, political, or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind.” This language mirrors the language adopted in the Declaration on the Inadmissibility of Intervention five years earlier. Similar language appears in the subsequent Charter on the Economic Rights and Duties of States and in multiple General Assembly Resolutions after 1970. All of the international instruments referencing non-intervention discuss both intervention using military force and intervention using coercion that does not involve the use of military force.

It is clear, then, that non-intervention applies not just to activities directly or indirectly involving force, but to other activities that “subordinate the sovereign will” of a state. The principle of non-intervention is sometimes applied to “economic coercion” and “political coercion.” Economic coercion occurs when a state takes actions that severely harm another state’s economy in order to change the policy of the target state. This type of coercion is most commonly understood to include unilateral economic sanctions. Discerning the acting state’s intent is central to the inquiry of whether economic coercion is present, as economically powerful states frequently take action that could be criminalized by a strict, effects-based standard of non-intervention. For example, the Organization of Petroleum Exporting Countries frequently raises and lowers its crude oil production in order to influence global supply, but such ac-


33. Id.

34. G.A. Res. 2131 (XX), ¶2, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (Dec. 12, 1965).


37. Id. at 349–54; see also, e.g., Final Act of the Conference on the Security and Cooperation in Europe, prin. VI, Aug. 1, 1975, 14 I.L.M. 1292 (1975).

38. Id.


tion is not condemned by the international community as a violation of non-intervention. Conversely, unilateral economic sanctions are frequently protested on the basis of non-intervention. Some have even argued that sudden cessation of foreign aid to a state when that state is heavily reliant on such aid can be a violation of non-intervention. It is worth noting, however, that Nicaragua alleged a violation of non-intervention in the *Nicaragua* case when the United States ceased providing aid to Nicaragua. The court rejected this contention.

Political coercion is even more difficult to define. This category of non-forcible intervention is typically applied to spreading propaganda across frontiers in order to incite violence. The International Covenant on Civil and Political Rights, an influential multilateral treaty, prohibits propaganda inciting war in Article 20(1). Material support of an internal political movement in violation of the target state’s domestic policy is also unlawful. Although these broad categories of political coercion are reasonably well-defined, the line between lawful diplomacy and unlawful political coercion is difficult to define. States frequently provide material support to opposition movements abroad without condemnation or without attempting to justify their actions. Scholars question whether the deployment of propaganda to incite war or rebellion deprives the target state of sufficient control so as to constitute coercion.

Therefore, the modern norm of non-intervention prohibits states from coercively interfering in the affairs of other states when the matter is one that the targeted state is entitled to decide freely. The bounds of the norm are relatively unclear, but the definition

---

47. Damrosch, *supra* note 29, at 45.
48. *Id.* at 13–21.
clearly includes several forms of state-to-state coercive activity. The effects-based nature of the non-intervention standard makes it an apt tool for assessing the international legality of cyber intrusions, even when such intrusions do not constitute uses of force.

Cyber Intrusions

The World Wide Web, or internet, was developed long after the formation of the customary form of non-intervention. Originally developed as a technology for the United States military, the precursor to the internet was formed in response to Cold War fears that the U.S. would not have an adequate communications network following a Soviet nuclear strike. These fears resulted in the creation of “ARPANET”—a network of interconnected U.S. government servers.

A number of ARPANET’s features continue to have effects on modern cyber intrusions. First, ARPANET transmitted data through the civilian telephone infrastructure already in place. Second, the government used a “packet switching” model of communication in which messages were divided into fixed segments rather than transmitted continuously. Third, the network was decentralized. Finally, ARPANET created a technology analogous to the router which sorted packets of data rather than letting them proceed unsorted to the main computers.

Later innovations modified ARPANET and turned it into the modern internet. DARPA soon needed an effective mechanism for enabling ARPANET to function across many different types of computers, which led to the adoption of the Transmission Control Protocol/Internet Protocol (TCP/IP) in 1983. The addition of TCP/IP to ARPANET’s previous infrastructure allowed the private sector and academia to innovate and expand the capability of the new network, which soon rendered ARPANET itself obsolete. These features also created the environment making DDoS attacks possible.

53. Gervais, supra note 50, at 529.
54. Id.
55. Id.
56. Waldrop, supra note 52, at 85.
57. Id.
“Cyber intrusion” covers a wide array of activities with varying severity and scope of effect. Other commonly used terms are “cyber attack” or “cyber exploitation,” both of which define slightly different forms of activity. Much of the language used in academic discussions of cyber intrusions is tied to authors’ discussions of the cyber intrusion as a use of force. This common approach to discussing cyber intrusions, attempting to draw an analogy with previous law regulating military force, results in a focus only on cyber intrusions severe enough to realistically be discussed as violations of the international prohibition on the use of force. This leaves out a wide array of online activity conducted by states. This has led to a number of scholars adopting the problematic position that there is no international legal regime capable of regulating cyber intrusions that do not rise to the level of uses of force.

The U.S. Army defines “cyber attack” as “the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. The definition also covers the intimidation of any person to further such objectives.” The Committee on Offensive Information Warfare defines “cyber attack” as efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them.

“Cyber exploitation” is used to describe cyber activity that seeks to gain confidential information from another state’s computer system or network. This type of intrusion is essentially a form of

58. Gervais, supra note 50, at 532.
60. Such as the subject of this Note, DDoS attacks causing no physical damage.
61. Russell Buchan, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, 17 J. CONFLICT & SECURITY L. 212, 213 (2012) (noting several scholars who have argued that cyber attacks which do not manifest physical damage are the subject of a gap in international law).
62. U.S. Army Training and Doctrine Command, Critical infrastructure threats and terrorism, in DCSINT HANDBOOK NO. 102, VII-2 (2006). Although this definition encompasses DDoS attacks with no manifested physical damage, the U.S. Army’s definition of cyber attack does not bear on the international law prohibition or permission of DDoS attacks.
63. COMM. ON OFFENSIVE INFO. WARFARE, NAT’L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10–11 (William Owens et al. eds., 2009) [hereinafter NRC REPORT].
64. Id. at 80; CYBERPOWER AND NATIONAL SECURITY 423–24 (Franklin D. Kramer et al. eds., 2009) (defining “cyber espionage” as “the unauthorized probing of a target computer’s configuration to evaluate its system defenses or the unauthorized viewing and copying of data files...”).
espionage because it focuses on obtaining information rather than causing destruction.\footnote{Gervais, supra note 50, at 533.} This activity vastly increases the amount of information states are able to obtain compared to previous forms of espionage—the costs and risks of gaining access to another state’s computers using domestic technology are comparatively low.\footnote{CYBERPOWER AND NATIONAL SECURITY, supra note 64, at 423–24.}

**DDoS Attacks**

This Note focuses on a particular form of cyber intrusion: the “distributed denial of service” (DDoS) attack. In a DDoS attack, an attacker attempts to prohibit a user from accessing a computer or a digital resource.\footnote{Felix Lau et al., Distributed Denial of Service Attacks, 3 2000 I.E.E.E. INTERNATIONAL CONFERENCE ON SYSTEMS, MAN, AND CYBERNETICS 2275, 2275 (2000).} DDoS attacks typically assume several forms. The first is an attempt to overload a network with activity by “flooding” the network with digital requests to use the resources.\footnote{Id.} This prevents a legitimate user from accessing the network.\footnote{Denial-of-Service Developments, CERT SOFTWARE ENG’G INST. (Jan. 3, 2000), http://www.cert.org/advisories/CA-2000-01.html.} This form of attack is the most common form of DDoS due to the ease of vastly increasing traffic on a foreign server, and the simple effectiveness of such a measure.\footnote{Id.} Other forms of DDoS attack include attempts to sever connections between two machines to prevent access, attempts to prevent an individual from using a service, or attempts to prevent access to service through a specific system.\footnote{Lau et al., supra note 67, at 2275.}

To conduct such an attack, the attacker creates a large number of programs that all engage with the target network.\footnote{Id.} This is done by controlling a number of software packages located throughout the internet to execute the program (the “Agent-Handler Model” of a DDoS attack) or through an Internet Relay Chat (I.R.C.) communication channel. The latter method is known as the “I.R.C.-Based Model.”\footnote{Stephen M. Specht and Ruby B. Lee, Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures, PROCEEDINGS OF THE 17TH INTERNATIONAL CONFERENCE ON PARALLEL AND DISTRIBUTED COMPUTING SYSTEMS, 2004 INTERNATIONAL WORKSHOP ON SECURITY IN PARALLEL AND DISTRIBUTED SYSTEMS 543, 543–44 (2004).} Thus, an attacker must create a master program that controls a number of agent programs, infiltrate the target network, and order the
master program to execute the agent programs. These agent programs directly attack the target resource, leading to the “denial of service.” The attack itself consists of multiple requests for information flowing from the agent programs to the targeted network or server, which overwhelms the system’s ability to sort packets of data.

Attacks can increase the efficacy of an attack by using “botnets.” A botnet is a group of computers which the attacker compromises and uses without the owner’s knowledge. Creation of a botnet enables an attacker to focus the resources of thousands of cooperating computers to send requests for information to a country’s web pages. This enables an attacker to overload a nation’s web infrastructure with relatively little resource expenditure. These attacks can have physically destructive consequences through disabling certain systems. But many of them manifest no physical damage.

DDoS attacks occur frequently in the international arena and the source usually remains unknown. The United States, in particular, has been the subject of a number of notable DDoS attacks since the 1990s. Following the 2002 Winter Olympics in Salt Lake City, several U.S.-based servers received DDoS attacks that appeared to originate in South Korea. In 1998, an attack, known as “Solar Sunrise,” broke through the Department of Defense’s security shield, apparently originating in the United Arab Emirates. This event illustrates one of the chief difficulties of tracking DDoS attacks—determining the perpetrator. Although the computers used in Solar Sunrise appeared to be in the United Arab Emirates, France, Taiwan,
and Germany, the attack was actually carried out by three high school students; one from Israel and two from California. The largest verified DDoS attack to date, discussed herein, occurred in 2007 on Estonia.

DDoS Attacks in International Law

DDoS attacks that cause no physical or financial damage are extremely difficult to analogize with previous activity regulated by the principle of non-intervention and the prohibition on the use or threat of force. The definitions of “armed force” and “intervention” evolved consistently with the technology available at the time, and there is very little consensus on what these terms mean with regard to new cyber techniques. The difficulty of attributing DDoS attacks to a state actor has led to a paucity of state practice on the issue. Previous scholarship has broadly focused on applying the prohibition of the use of force to cyber attacks. Even scholarship arguing for the application of the principle of non-intervention to cyber warfare has not specifically addressed DDoS attacks in detail.

Attribution

One difficulty with holding states accountable for DDoS attacks is the problem of attribution. Many such attacks are carried out using surrogates, individuals not directly associated with the acting state or organization, domestically or abroad. An internationally wrongful act can only be attributed to a state if the act was carried out by the authorities of that state, or by agents under the direction and control of that state. The question of indirect action violating international law was the issue considered by the I.C.J. in Nicaragua. The court in that case attempted to establish a high threshold of force

84. Shackleford, supra note 80, at 205.
85. See, e.g., Buchan, supra note 61, at 226 (briefly discussing the DDoS attack on Estonia but focusing primarily on a concept of non-intervention involving inducement to a particular political act rather than a subordination of the sovereign will of a state through creation of widespread disruption).
necessary to justify self-defense under international law, and was thus reluctant to acknowledge less severe forms of indirect action as violations of Article 2(4). This decision greatly restricted the application of Article 2(4) to covert warfare using surrogates and unconventional means, which has had lasting effects on the interpretation of the rule and its application to cyber activities.

Determining whether a particular state has sanctioned or implemented a DDoS attack can be difficult. Attacks using botnets can often connect hijacked computers from across the globe, making the search for the original executor of the master program nearly impossible. Modern cyber attackers are able to “spoof” credentials to gain access to networks, allowing the attackers to utilize a computer network without the owner’s consent or even without the owner’s knowledge.

The difficulty of obtaining accurate information on the perpetrators of cyber attacks is illustrated by the DDoS attack on Estonia. The question of who bore the responsibility for directing or encouraging the attacks was never conclusively answered. Some evidence suggests that Russia encouraged civilian hackers to attack Estonia, but Russian officials denied being involved. Similarly, in the recent infiltration of Sony allegedly carried out by North Korea-sanctioned operatives, the attackers used a network of proxy servers in Thailand, Poland, and several other countries. The reliance on semi-private hackers affiliated only loosely with national governments enables those governments to plausibly deny involvement in

90. See Cooke, supra note 76; TIKK ET AL., supra note 78.
91. For a comprehensive overview of methods of maintaining anonymity in cyber-attacks and the technical difficulties in tracing attackers for purposes of attribution, see Mauno Pihelgas, Back-Tracing and Anonymity in Cyberspace, in Peacetime Regime for State Activities in Cyberspace 40, 48 (Katharina Ziolkowski ed., 2013).
92. NRC REPORT, supra note 63, at 173.
93. Charles Clover, Kremlin-Backed Group Behind Estonia Cyber Blitz, Fin. Times (Mar. 11, 2009), http://www.ft.com/intl/cms/s/0/57536d5a-0dcd-11de-8ea3-0000779fd2ac.html#axzz45x9EgzbX.
94. NRC REPORT, supra note 63, at 173.
DDoS attacks. This type of warfare is similar to the proxy wars of a different kind fought by powers during the Cold War using surrogates in Latin America and Asia. Cyber warfare carries the same advantages for states today as covert support of guerrilla warfare did during the Cold War.

Support in Customary Law

Upon solving the attribution problem, another problem is determining whether the requisite state practice and accompanying opinio juris exist to support the notion that non-destructive DDoS attacks violate the norm of non-intervention. In order for this prohibition to reach the status of a customary norm, it must be supported by “widespread and consistent” state practice, which can be shown through states’ actions and statements. That practice must also be accompanied by opinio juris, meaning states must be acting in this way out of a sense of legal obligation.

The first problem with establishing this norm as custom is the aforementioned attribution problem that makes DDoS attacks attractive to aggressive governments. Although, as stated earlier, attributing DDoS attacks to a particular state can be difficult, reasonably reliable data indicates that states carry out DDoS attacks causing no physical damage quite frequently, with very little protest or condemnation from the international community. However, the fact that a number of states do not conform to a customary norm does not preclude such a norm from existing, though it may provide evidence that a norm is often violated.

Expanding Article 2(4) to include cyber activities unaccompanied by physical damage similar to the damage caused by traditional armed force, an expansion which would enable categorization of non-destructive DDoS attacks as “force,” has gained little traction.

97. Waxman, supra note 89, at 447.
98. Id. at 448.
100. Id.
101. Even the large attack on Estonia in 2007 was not condemned by NATO or the United States. Shackleford, supra note 80, at 209–10.
in international law. The difficulty of expanding this definition is demonstrated by the status of “economic coercion” in customary law. Economic coercion involves deliberate action taken by a state to change policy in another state by promising economic harm if the policy demand is not met. Economic coercion, like DDoS attacks, can be incredibly disruptive. Yet, it does not involve the direct physical harm of military force. At the U.N. Charter’s drafting, several states unsuccessfully proposed including economic coercion in the U.N. Charter’s definition of “force.” Throughout the U.N. Charter’s history, a number of states—mostly developing states and former Soviet Bloc states—have asserted that “force” under the U.N. Charter is broader than military force and includes economic coercion, but this idea has met with considerable pushback from Western states, who still interpret Article 2(4) as only prohibiting military force.

Economic coercion is still not considered a violation of the U.N. Charter. The court in Nicaragua did address the question of economic coercion, but determined that the U.S. trade embargo and cessation of aid to Nicaragua did not amount to a use of force under international law. Nevertheless, some states and scholars frequently assert that Article 2(4) of the U.N. Charter has been violated when other states take economic action in order to induce compliance with a demand.

Although the international community has not accepted economic coercion as “force” under customary international law, acceptance is growing for the idea that digital attacks may qualify as force if they cause physical damage. Scholars vary on the degree to which such a prohibition has come into effect. One problem

103. See Waxman, supra note 89, at 426–37; See also Tallinn Manual, supra note 8, Rule 11, ¶¶ 3–9 (articulating factors for determining whether cyber-activities qualify as uses of force).


109. See supra Introduction.

110. See, e.g., Anthony D’Amato, International Law, Cybernetics, and Cyberspace, 76
with asserting that non-destructive DDoS attacks can violate non-intervention is the murky nature of the non-intervention norm, but pursuing agreement on this issue through a non-intervention framework appears more likely than doing so through a use of force framework. It is also evident that formulating international agreement regarding cyber attacks will be very difficult. This is driven by the difficulty of regulating international cyber activities, and by the hugely divergent strategic interests of state actors in this realm.

The effects of a non-destructive DDoS attack are analogous to economic coercion. The effects of a DDoS attack are more attenuated than they are for physical or military force. The detriment to the target state comes from the inability of legitimate users to access digital resources, which can affect the economic and political health of a target state. Similarly, economic coercion has an economic effect on the target state which is not an immediate result of the economic measures taken.

THE BENEFITS OF A NON-INTERVENTION FRAMEWORK FOR NON-DESTRUCTIVE DDoS ATTACKS

Non-destructive DDoS attacks are permitted by international law, but are unlawful if they are coercive. The prohibition on the use or threat of force is insufficient to address DDoS attacks without immediate physical effects, but the principle of non-intervention adequately addresses them. Regardless of whether a specific policy goal is being pursued by the attacking state, DDoS attacks causing widespread disruption of communications and digital functionality violate international law.

Inadequacy of Article 2(4)

The international legal regime surrounding Article 2(4) of the U.N. Charter is likely adequate to address DDoS attacks that cause

---

111. See Gerhard Hafner, Present Problems of the Use of Force in International Law: Intervention by Invitation, 2009 INST. DE DROIT INT’L YEARBOOK 299, 309 (“Hardly any other expression used in international law is as vague, blurred, controversial, and disputed as the term “intervention.”).  

112. Waxman, supra note 89, at 425.  

113. Id. at 425–26.
physical damage. International law is developing quickly to recognize Article 2(4) as an effects-based prohibition and is applying that framework to cyber warfare. Due to societal reliance on networked information systems, a DDoS attack on a vital network could have similar effects on human life and property to the launch of a missile. DDoS attacks could shut off heat for an entire region during a cold winter or disable a power grid. However, many DDoS attacks have no immediate physical effects.

The Article 2(4) prohibition on the use of force is clearly inadequate to address non-destructive DDoS attacks. Although the aforementioned effects of a DDoS attack can have significant consequences for the target state, the difficulty of applying Article 2(4) even to attacks manifesting physical damage renders application to attacks manifesting no physical damage impossible. The principle of non-intervention is much more useful in attempting to establish international legal responsibility to indirect actions taken by states.

**Analogy to Political and Economic Coercion**

Non-destructive DDoS attacks can more accurately be analogized to political or economic activities violating the principle of non-intervention. Although such activities are frequently carried out by states, they violate the principle of non-intervention when they become coercive. Such activities involve support for groups or causes within states, and although they frequently cause no physical destruction or consequences, the key component of their illegality is the subordination of the target state’s sovereign will.

Coercion can be present even if no physical damage occurs, as it is with political and economic coercion. DDoS attacks can have widespread effects on the ability of a state’s people to interact with others online for a period of time or prevent them from accessing certain information. This is frustrating the sovereign will of the target state by preventing communication or information sharing that the target state would like its citizens to engage in. This type of harm is

118. *Id.* at 371.
similar to the harm resulting from political coercion, which sometimes consists of sending information into a country in support of a political movement. If adding information to a state’s internal discourse against its will can qualify as a violation of non-intervention, then halting the spread of information within a country must qualify as well.

A potential problem with analogizing non-destructive DDoS attacks to economic coercion is the relatively weak status of economic coercion in international law. However, the case for large scale DDoS attacks as violations of non-intervention is stronger than that of economic coercion. This is because of the discernible intent of the acting state and because of the possibility of lawful intentions that exist in the case of economic coercion but not DDoS attacks.

The concept of economic coercion declares a state’s otherwise lawful actions unlawful because of their effects and intentions. States engaging in acts with the effects of economic coercion can have lawful intentions, such as OPEC’s manipulation of oil supply to influence the global price of crude oil. Furthermore, states have broad discretion in their economic and foreign policy under customary law, though this discretion is sometimes limited by treaty obligations. Thus, actions decried by victim states as economic coercion are frequently considered lawful by the international community.

In contrast, states do not have the affirmative right under customary international law to target foreign states’ computer systems, though it could be argued that the lack of a prohibition of such behavior grants states that right. Furthermore, DDoS attacks with effects severe enough to be protested by target states will not have a discernible intent that is within the acting state’s sovereign rights.

120. INTERNATIONAL LAW 333–34 (Richard Falk et al. eds., 5th ed. 1972); see also Damrosch, supra note 29, 15–16.
121. Farer, supra note 41, at 407.
123. See Boorman, supra note 42.
124. See generally STATES AND SOVEREIGNTY IN THE GLOBAL ECONOMY (David Smith, Dorothy Solinger & Steven Topik eds., 1999).
126. This would be an argument on the basis of the so-called “Lotus Principle,” which dictates that if an act is not prohibited by international law, it is permitted. See Anthea Roberts, Traditional and Modern Approaches to Customary International Law: A Reconciliation, 95 Am. J. Int’l L. 757, 776 (2001).
To illustrate the coercive nature of a non-destructive DDoS attack, consider the example of an attack on a university computer network. Such an attack can halt research, prevent teachers from communicating with students, and prevent students from sending assignments via email. Such an attack could prevent scientists from completing potentially life-saving research on time, and could at the very least diminish real-world capability in some field due to slowing technological development at the university. In order to carry out an effective attack of this nature, the attackers would likely use botnets comprising private machines from many different locations.

For a real world example of the effects of a widespread DDoS attack with no physical destruction, consider the case of the 2007 DDoS attack on Estonia. This attack, a “flooding” style DDoS attack, occurred in two waves. First, the attackers bombarded public and private Estonian websites and computers with fake requests for information from April 27, 2007 to May 2, 2007. This attack caused the websites of the Prime Minister, the President, the Parliament, and several daily newspapers to crash. Second, on May 9, a DDoS attack using a botnet shut down the online portal of the largest Estonian bank, and smaller-scale assaults continued for the following weeks of May. The lack of functionality of Estonia’s main news outlets essentially prevented it from telling the world about the attack while it was occurring. The attack also targeted computers used in telephone exchanges, which could have resulted in widespread loss of telephone functionality across the country. During this period,

---

127. Such an attack occurred on the University of Minnesota’s computers in 1999, widely considered to be the first major DDoS attack against a university. See Lee Garber, Denial of Service Attacks Rip the Internet, IEEE COMPUTER SOC’Y (Apr. 4, 2000), http://www.computer.org/csdl/mags/co/2000/04/r4012.pdf.

128. Schmitt, supra note 10, at 916 (discussing a computer network attack disrupting a university’s military-related research, which eventually leads to diminished capability on the battlefield causing injury or loss of life).


130. Id.


133. See Kelsey, supra note 79, at 1429 (describing the effects of targeting “mission-critical” computers and networks in a state).
there were at least 128 unique DDoS attacks targeting Estonian internet protocols.\textsuperscript{134} World powers took note of the attack, which illustrated that a highly developed online infrastructure can be a detriment to a state as well as a benefit.\textsuperscript{135}

The perpetrators of the attacks are still not conclusively identified. As is common with a DDoS attack, the computers used in the attack were located all over the world.\textsuperscript{136} Reports surfaced that users on Russian-language websites were goaded into attacking Estonian websites through chatrooms.\textsuperscript{137} The major botnet blitz took place on May 9, a national patriotic holiday in Russia.\textsuperscript{138} Following the attacks, a U.S. government report concluded that politically motivated hacker gangs were responsible and that Russian security agencies were not directly involved.\textsuperscript{139} In contrast, the Estonian government and a number of prominent internet operatives in Russia stated their belief that Russia at least gave its blessing to the hackers, and possibly facilitated their attack.\textsuperscript{140}

Although such attacks as the hypothetical DDoS attack on the university or the large-scale DDoS attack on Estonia are not as immediately harmful as an attack amounting to force, the consequences of such an attack are similar to consequences of other activities often noted as violations of non-intervention. Furthermore, such attacks violate non-intervention even without a clear inducement to a policy change purely because of their effects on a state’s digital network.

The attacks were carried out by independent agents, whose activities may have been encouraged and facilitated by the state. Such attacks can be used fairly easily to extort a network-reliant state, and DDoS attacks are already a common tool for extortion between individuals in the private sector.\textsuperscript{141} An attack such as the one conducted against Estonia, although manifesting no physical destruction, had a sufficient effect on Estonia to constitute a subordination of its sovereign will. The government of Estonia wanted its citizens to

\begin{itemize}
  \item \textsuperscript{136} Shackleford, \textit{supra} note 80, at 206.
  \item \textsuperscript{137} See Landler & Markoff, \textit{supra} note 131.
  \item \textsuperscript{138} Davis, \textit{supra} note 132.
  \item \textsuperscript{139} Waterman, \textit{supra} note 136.
  \item \textsuperscript{140} \textit{Id}.
  \item \textsuperscript{141} Susan Brenner, \textit{At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare}, 97 J. CRIM. L. & CRIMINOLOGY 379, 384–86 (2007).
\end{itemize}
have access to government web sites and to bank accounts.\textsuperscript{142}

Applying the coercion standard of non-intervention to the attack on Estonia accurately prohibits DDoS attacks without needing to define them as uses of force. The attack is a twenty-first century example of the situation at hand in the \textit{Nicaragua} case. Indirect means were used to influence a state, leaving the perpetrators difficult to identify. Although there was no physical destruction such as existed in \textit{Nicaragua}\textsuperscript{143} there was widespread disruption that had the potential to cause widespread harm. Interference with a foreign government’s communications and electronic banking infrastructure must qualify as “dictatorial” interference,\textsuperscript{144} even if it does not constitute force.

CONCLUSION

Approaching non-destructive DDoS attacks through the non-intervention framework facilitates an assessment of potential violations of international law involving state-sanctioned DDoS attacks. Given the widespread disruptive power of these attacks and the obvious state dislike of being the victim of such an attack, it allows for an analysis that acknowledges the wrongfulness of such conduct without rising to the level of a violation of Article 2(4). This way, the difficulty of attempting to analogize DDoS attacks to physical force can be avoided.

Using the framework of non-intervention also avoids waiting for developments in international law that may never come. Existing international law is adequate to police DDoS attacks without requiring the establishment of an entirely new global legal regime. It also enables international legal scholarship to apply a normative framework to DDoS attacks without requiring adoption of a view that is not supported by state practice.

More development in this field is necessary before the non-intervention framework as applied to non-destructive cyber attacks becomes a firmly established norm of customary international law. Although a multilateral treaty seems unlikely, scholars are already discussing alternatives to Article 2(4) to apply to non-destructive

\textsuperscript{142} Although the will of a state’s government is not always perfectly synonymous with the “sovereign will” of that state, in this instance I use the government’s views as the closest proxy of sovereign will.


\textsuperscript{144} See supra text accompanying note 23.
cyber attacks. It is likely that non-intervention will continue to expand in application to DDoS attacks without physical effects, just as customary law has continued to expand with technology in the past.

William Mattessich*

* Managing Editor, Columbia Journal of Transnational Law; J.D. Columbia Law School 2016; B.A. University of Iowa 2012. The author is grateful to Professor Eben Moglen for his assistance in writing this Note and Professor Matthew Waxman for his advice on the international legal framework surrounding Article 2(4) of the U.N. Charter. The author also wishes to thank Victoria Gilcrease-Garcia, David Menon, and Henry Ross for their assistance with background research into various aspects of the international law of cyberspace.