Brooklyn Journal of International Law

Volume 36
Issue 3
SYMPOSIUM:
Governing Civil Society: NGO Accountability,
Legitimacy and Influence

Article 11

2011

Cyberattack Attribution Matters Under Article 51 of the U.N. Charter

Levi Grosswald

CYBERATTACK ATTRIBUTION MATTERS UNDER ARTICLE 51 OF THE U.N. CHARTER

> "[N]onstate actors . . . are able to organize into . . . networks . . . more readily than [] traditional, hierarchical, state actors . . . . [W]hoever masters the network form stands to gain the advantage."[1]

INTRODUCTION

Day 1: An anonymous online group posts a message instructing the United States ("U.S.") to close all overseas bases within six days or else suffer destruction of major U.S. infrastructure.

Day 6: Twenty-two hydroelectric dams and power plants along the West Coast are remotely shut down, severing electricity and phone service throughout the western United States. Thirty-five deaths are reported in one day, ranging from traffic accidents to heart attacks and heatstroke among the elderly. Reports emerge that an unpowered dam in California broke, killing thousands.

Day 9: The U.S. air-traffic control system is sabotaged, freezing radar screens and scrambling information among close-flying planes. After a midair collision kills almost 500 people, all commercial flights are grounded. Economic loss from the groundings amounts to billions daily.

Day 12: A computer-controlled chemical factory in Detroit blows up, destroying the eastern half of the city. After reviewing circumstantial evidence, the military suspects Russia and China are the masterminds. Both countries deny any involvement.

Day 20: The United States retaliates physically while covert cyberattacks shut down both Russian and Chinese power grids. Oil pipelines in both countries are disrupted. Transportation, financial and power systems are shut down, causing immeasurable economic damage. Reports indicate that the number of Russian and Chinese deaths far outnumber those suffered in the United States.

Day 25: After the attacks subside, U.S. Information Warfare Command obtains user identification data from the West Coast attacks. The data is traced back to civilian-led liberation groups in the Republic of Abkhazia. Attackers merely routed strikes through Russian and Chinese networks to provide the illusion of hostility toward the United States.

---

1. Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 76 (2004) [hereinafter Brenner, *Toward a Criminal Law*] (quoting David Ronfeldt & John Arquilla, *Networks, Netwars, and the Fight for the Future*, 6 FIRST MONDAY 10, Oct. 2001), *available at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/889/798.

> Day 26: In a public apology to Russia and China, the President says, "We are all victims." That may be, but it seems the people of both nations have paid a higher price for the United States' mistake.[2]

This is the new reality. Cyberattacks and information-systems warfare are no longer fictional concepts posing as a concern for some far-off generation.[3] Private, public, and military systems infrastructures are vulnerable to cyberattacks worldwide.[4] Attacks are not limited to the United States, as a great number of countries have been targeted.[5] Many of the

---

2. John Arquilla, *The Great Cyberwar of 2002*, WIRED (Feb. 1998), http://www.wired.com/wired/archive/6.02/cyberwar_pr.html.

3. Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?*, 22 HOUS. J. INT'L L. 223, 226 (2000).

4. For example, Google's password system was the target of a cyberattack in January 2010 that resulted in the theft of Google's intellectual property. Jonathan Stempel, *Google Cyber Attack Hit Password System: Report*, REUTERS (Apr. 20, 2010), http://www.reuters.com/article/idUSTRE63J0BO20100420. In 2009, cyberspies infiltrated the U.S. electrical grid and implanted programs that could disrupt the system. Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J. (Apr. 8, 2009), http://online.wsj.com/article/SB123914805204099085.html. The United States' military network of "2.1 million computers and 10,000 local area networks (LANs) . . . are probed by outsiders about five hundred times a day." Aldrich, *supra* note 3, at 228–29 (citing Douglas Waller, *Onward Cyber Soldiers*, TIME, Aug. 21, 1995, at 38, 39).

5. *See* Robert Coalson, *Behind The Estonia Cyber Attacks*, RADIO FREE EUR. RADIO LIBERTY (Mar. 6, 2009), http://www.rferl.org/content/Behind_The_Estonia_Cyber attacks/1505613.html (discussing the 2007 cyberattack that blocked Estonia's websites, paralyzing the country's Internet infrastructure and freezing bank cards and cellular phone networks); *see also* Associated Press, *A Look at Estonia's Cyber Attack in 2007* (July 8, 2009), http://www.msnbc.msn.com/id/31801246 ("Experts said hundreds of thousands of computers were used in a coordinated attack against government agencies and banks."); Matthew Weaver, *Cyber Attackers Target South Korea and US*, GUARDIAN.CO.UK (July 8, 2009), http://news.bbc.co.uk/2/hi/technology/8139821.stm (discussing the cyberattack against South Korea's presidential Blue House, defense ministry, national assembly, Shinhan bank, and Korea Exchange bank); Dan Goodin, *Georgian Cyber Attacks Launched by Russian Crime Gangs*, THE REGISTER (Aug. 18, 2009), http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/ (The cyberattack, which targeted e-commerce sites and Georgian government sites, "coincided with the Russian military's invasion of Georgia in August 2008."). It is not just the United States that fears cyberattacks from actors based in foreign countries. According to a 2009 McAfee survey, a plurality of global companies fear cyberattacks from U.S.-based actors more than foreign-based actors. *See* Robert Lemos, *Cyber Attacks from U.S. "Greatest Concern,"* SECURITYFOCUS (Jan. 28, 2010), http://www.securityfocus.com/print/brief/1066 ("The survey found that 36 percent ranked network attacks from the United States as their "greatest concern," compared to 33 percent most concerned about attacks from China. Russia came in a distant third, with only 12 percent of those polled rating it the most concerning."). For the report based on the study, see Stewart Baker, Shaun Waterman & George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*,

actors executing or participating in these attacks will be nonstate, and in extreme cases, stateless.[6]

Attribution is the means by which responsibility for illegal acts or omissions are attached to the state.[7] Vincent-Joël Proulx[8] described the need for eliminating the concept of international state attribution and holding a state strictly liable if it fails to prevent terrorists from launching an attack within its borders.[9] Although this seems contradictory to the United Nations ("U.N.") Charter, Proulx argued that this notion is in fact supported by the international community's objective of eradicating terrorism.[10]

MCAFEE, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf (last visited on Dec. 21, 2010).

6. Ronfeldt & Arquilla, *supra* note 1.

7. Amanda Tarzwell, Note, *In Search of Accountability: Attributing the Conduct of Private Security Contractors to the United States Under the Doctrine of State Responsibility*, 11 OR. REV. INT'L L 179, 192 (2009).

8. Proulx received LL.L. and LL.B. degrees from the University Ottawa and an LL.M. in International Legal Studies at New York University School of Law. *Former Clerks*, MCGILL CTR. FOR HUMAN RIGHTS & LEGAL PLURALISM, http://www.mcgill.ca/humanrights/clinical/clerkships/formerclerks/ (last visited Dec. 21, 2010). Proulx is currently pursuing a doctoral degree in international law at McGill University. *Id*. Proulx's dissertation surveys the relationship between international state responsibility and terrorism, with a focus on human rights and international relations. *Id*.

9. Vincent-Joël Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L L. 615, 643–53 (2005). It should be noted that there is no international agreement as to the definition of terrorism. *Id*. at 647; *see also* Vincent-Joël Proulx, *Rethinking the Jurisdiction of the International Criminal Court in the Post-September 11th Era: Should Acts of Terrorism Qualify as Crimes Against Humanity*?, 19 AM. U. INT'L L. REV. 1009, 1030–41 (2004) (discussing "terrorism" as having an international nature). Determining what constitutes cyber terrorism is particularly difficult. *See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 382–405 (2007) [hereinafter Brenner, *Attribution and Response*]. Professor Brenner, in short, defines cybercrime and cyberterrorism as the use of computer technology to commit a crime or engage in terrorist activity, respectively. *Id*. at 382, 386. Although terrorism is thought of as a type of crime, Professor Brenner distinguishes those concepts in that "crime is personal while terrorism is political." *Id*. at 387. She then distinguishes cyberterrorism from cyberwarfare in that terrorism is intended to "demoralize a civilian population," while warfare is "not supposed to target civilians." *Id*. at 387–88.

10. Proulx, *supra* note 9, at 643–53. On September 12, 2001, the U.N. General Assembly passed a resolution calling for "international cooperation to prevent and eradicate acts of terrorism" and holding "those responsible for aiding, supporting, or harbouring the perpetrators, organizers and sponsors of such acts . . . accountable." *Id.* (quoting G.A. Res. 56/1, U.N. GAOR, 56th Sess., 1st mtg. U.N. Doc. A/Res/56/1 (2001)). The U.N. Charter is a treaty signed and ratified by 192 states with the express purposes of "maintain[ing] international peace and security, . . . [and] develop[ing] friendly relations among nations based on respect for the principle of equal rights . . . ." U.N. Charter art. 1, para.

Attributing responsibility to a state for an attack is guided by two diverging concepts—direct and indirect responsibility.[11] Under direct responsibility, a state may be held liable if its direct act or omission led to harm, if a group or actor acts as a state agent, or if a state has "control" over a nonstate actor.[12] Indirect responsibility is more opaque and appears when there is no underlying link between an actor and a state.[13] Assigning direct liability for an attack is difficult if a state has no ties to terrorist activities occurring in its territory.[14] As such, the indirect liability analysis shifts to a focus on the host-state's duty to prevent terrorist attacks from emanating from within its territory.[15] A state's apathy or disregard for terrorist activity within its territory triggers its responsibility as though it had directly participated in the attack.[16] Given the enorm-

---

1, 2. Furthermore, the U.N. Charter requires members to "settle their international disputes by peaceful means in such a manner that international peace and security . . . are not endangered." *Id.* art. 2, para. 3.

11. Proulx, *supra* note 9, at 623–26. Proulx refers to this as the "direct/indirect dichotomy." *Id*. at 623.

12. *Id*. at 624; *see also* Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27) [hereinafter Nicaragua] (holding a state legally responsible for the acts of nonstate actors if it had "effective control" over them); Prosecutor v. Tadic, Case No. IT-94-1-A, I.C.T.Y. App. Ch., at 49 (July 15, 1999) [hereinafter Tadic] (holding a state legally responsible for the acts of organized armed groups when the state had "overall control" over them). As Professor Proulx points out, "the issues surrounding direct state responsibility are relatively clear and require no further discussion here." Proulx, *supra* note 9, at 624.

13. *Id*. at 624. Professor Proulx's notion of indirect responsibility is consistent with the concept of "vicarious responsibility." *Id*. at n.43; *see also* Davis Brown, *Use of Force Against Terrorism After September 11th: State Responsibility, Self-Defense and Other Responses,* 11 CARDOZO J. INT'L & COMP. L. 1, 13 (2003) ("The difference between [direct] responsibility and vicarious responsibility is that in the former, responsibility flows from the injurious acts, and in the latter, responsibility flows from the failure to take measures to prevent or punish the act.").

14. Proulx, *supra* note 9, at 624.

15. *Id*. The focus of the analysis is still whether the state breached an international obligation. However, under indirect responsibility the breach will likely consist of an omission, intentional or unintentional, as opposed to an act. *Id*.; *see, e.g.,* John Bellinger, Legal Advisor to the U.S. Sec'y of State, Legal Issues in the War on Terrorism, Address Before the London School of Economics (Oct. 31, 2006), *in* 8 GERMAN L.J. 735, 739 (2007) ("As a practical matter . . . a state must be responsible for preventing terrorists from using its territory as a base for launching attacks. And, as a legal matter, where a state is unwilling or unable to do so, it may be lawful for the targeted state to use military force in self-defense to address that threat.").

16. Proulx, *supra* note 9, at 624; *see also* DANIEL BYMAN, DEADLY CONNECTIONS: STATES THAT SPONSOR TERRORISM 219 (2005) (noting the "great[] contribution a state can make to a terrorist's cause [by] not act[ing] against it").

ous impact nonstate actors have on international peace, such a broadening of state responsibility is not unreasonable.[17]

State responsibility depends on attribution.[18] Attribution is not only a necessary factor in determining whether a state has violated international law, it is also used to determine whether a victim-state may take action against the perpetrating state.[19] Nonstate actors, whose nature and class place them outside the definition of a state, increasingly perform modern acts of aggression.[20] By expanding states' duties to monitor and restrain nonstate actors, the international community permits imposing liability on states for failing to prevent acts not traditionally attributable to them.[21]

This Note theorizes that, within the ambit of cyberattacks and cyberterrorism, the concept of state attribution must not be eliminated. Not only must cyberattack attribution remain in place, it should be reinforced and enhanced through increased state cooperation and collaboration. The Internet provides virtually everybody with the opportunity to disguise one's online persona, erase one's digital tracks, and transfer evidence onto innocent computers.[22] In order to ensure that it is not retaliating against an innocent state, a victim-state must correctly attribute an attack to the actual attacker. Identifying a cyberattacker is essential to determining the nature of an attack.[23] Determining the nature of an attack is generally the first step in developing a response, whether it is political, domestic, or military, to ensure that it does not violate Article 51 of the

---

17. Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F.L. REV. 65, 89 (2009); *see also* Anne Petitpierre, Vice-President, Int'l Comm. of the Red Cross, Opening Address at the Bruges Colloquium: Relevance of International Humanitarian Law to Non-State Actors (Oct. 30, 2002), *available at* http://www.cicr.org/eng/resources/documents/misc/5f8jez.htm ("In all areas of international relations—economics, ecology, politics, military affairs—non-State actors, be they infra- or supra-State, have assumed increasing importance and have asserted themselves as international players that cannot be ignored.").

18. Berglind Halldorsdottir Birkland, Note, *Reining in Non-State Actors: State Responsibility and Attribution in Cases of Genocide*, 84 N.Y.U. L. REV. 1623, 1630 (2009).

19. *Id.* at 1630–31; *see also* Jorn Greibel & Milan Plucken, *New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia*, 21 LEIDEN J. INT'L L. 601, 604 (2008) (explaining that state attribution leads to significant consequences, in particular, that "the victim state [may also] take measures in reaction to the violation").

20. Michael Anderson, Note, *Reconceptualizing Aggression*, 60 DUKE L.J. 411, 411 (2010).

21. Birkland, *supra* note 18, at 1626.

22. Meiring de Villers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 419, 459–60 (2008).

23. Brenner, *Attribution and Response*, *supra* note 9, at 405.

U.N. Charter.[24] As such, attribution is an issue that should not be circumvented.

Part I of this Note examines Articles 2(4) and 51 of the U.N. Charter and the evolution of international jurisprudence attributing legal responsibility to a state for the acts of nonstate actors, as it is important to understand how states became responsible for the acts of nonstate actors. Part II will analyze the inherent difficulties in determining the identity and location of a cyberattacker, the nature of a cyberattack, and why state attribution in the cyberattack context is a necessary part of the analysis. Part III will consider increased state cooperation and collaboration as a means of reinforcing attribution.

I. THE U.N. CHARTER ON USE OF FORCE AND THE RIGHT TO SELF-DEFENSE

After World War II, world leaders created the U.N. in an attempt to fashion an international legal system that would foster enduring peace.[25] Article 2 of the U.N. Charter, the U.N.'s founding document, addresses the standards by which member states pursue international peace and security.[26] In particular, Article 2(4) completely limits a state's ability to use unilateral force,[27] stating "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[28] This seemingly total repudiation of force, however, is balanced by an important exception, the well-settled principle of the right of self-defense.[29]

A. The Self-Defense Doctrine under Article 51

Article 51 provides that "[n]othing contained in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."[30] Although Article 51 permits individual self-

---

24. *Id*.

25. Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 215 (2002).

26. *Id*. at 216.

27. *Id*.

28. U.N. Charter art. 2, para. 4.

29. Jensen, *supra* note 25, at 216. Another important exception exists to Article 2(4)'s repudiation of force: collective military action authorized by the U.N. Security Council. *Id*. This exception is outside the scope of this Note and will not be discussed.

30. U.N. Charter art. 51.

defense, it is limited by the principles of necessity and proportionality.[31] Necessity refers to the requirement of self-defense under the circumstances because settlement or resolution could not be acquired by peaceful means.[32] On the other hand, proportionality limits self-defense actions to "the amount of force necessary to defeat an ongoing attack or to deter future aggression."[33] The doctrines of necessity and proportionality are considered to be customary standards that states responding in self-defense need to abide by.[34]

The self-defense doctrine's core principle is that a state may only act in self-defense in response to an "armed attack."[35] This concept is a widely accepted foundation in international law. However, the quantity and

---

31. Jensen, *supra* note 25, at 218 (citing Nicaragua, *supra* note 12).

32. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyber Attacks: A Justification for the Use of Active Defenses Against States who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 32 (2009) (citing YORAM DINSTEIN, WAR, AGGRESSION, AND SELF-DEFENSE 87, 237 (4th ed. 2005)); *see also* Ian Johnstone, *The Plea of "Necessity" in International Legal Discourse: Humanitarian Intervention and Counterterrorism*, 43 COLUM. J. TRANSNAT'L L. 337 (2005).

33. Sklerov, *supra* note 32, at 32–33 (citing Michael Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 532 (2003)).

34. Gina Heathcote, *Article 51 Self-Defense as a Narrative: Spectators and Heroes in International Law*, 12 TEX. WESLEYAN L. REV. 131, 135 (2005). The concept of proportionality requires that defensive actions are limited to the region of the armed attack and not beyond the termination of conflict. *Id*. Proportionality should be viewed in terms of the defensive military campaign as a whole, rather than in terms of the difference of hostilities. *Id*. at 136.

35. Sklerov, *supra* note 32, at 31. Whether a cyberattack can constitute an "armed attack" is an issue beyond the scope of this Note, but is important enough to warrant a brief discussion. In order to determine what constituted an international armed conflict under Common Article 2 of the 1949 Geneva Conventions, Jean Pictet determined force of "sufficient scope, duration, and intensity" is deemed an armed attack. David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 90 (2010) (internal quotation marks omitted). As international law has evolved, three models have arisen that apply Pictet's criteria to modern uses of force. *Id*. at 91. The first is an "instrument-based approach" which assesses whether the harm produced by the cyberattack could only have been previously caused by a physical attack. *Id*. (internal quotation marks omitted). The second is an "effects-based approach" which only considers the overall effect of the cyberattack on the victim state. *Id.* (internal quotation marks omitted). Relation to a physical attack is not considered at all in the effects-based approach. *Id*. The third approach is one of "strict liability" which automatically deems any cyberattack against "critical national infrastructure" as an armed attack. *Id.* (internal quotation marks omitted). While these various approaches have been widely debated, all three models agree with the conclusion that a cyberattack can be deemed as an armed attack. *Id.* at 91–92; *see also* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 185–87 (2006).

quality of force required to constitute an armed attack has been the subject of ongoing debate.[36] This classification problem is likely exacerbated by the fact that neither the U.N. Charter nor the U.N.'s Definition of Aggression resolution[37] actually defines armed attacks.[38] This debate becomes quite nuanced as it pertains to cyberattacks, which are often viewed as "a use of force short of armed force."[39]

Although the definition of armed attacks under Article 51 is open to debate, it is clear that states invoking the doctrine of self-defense have prepared for armed attack by states, not nonstate or private actors, since the drafting of the Charter.[40] Article I of the Definition of Aggression[41]

---

36. Sklerov, *supra* note 32, at 31. *See generally* Sean D. Murphy, *Terrorism and the Concept of "Armed Attack" in Article 51 of the U.N. Charter*, 43 HARV. INT'L L.J. 41 (2002).

37. Definition of Aggression, G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974). An express purpose of the U.N. Charter is to "take . . . effective . . . measures for the suppression of acts of aggression or other breaches of peace." U.N. Charter art. 1, para. 1. The 1974 Definition of Aggression was an attempt by the U.N. General Assembly to provide normative guidance to the U.N. Security Council as to what constitutes an act of aggression. Sergey Sayapin, *A Great Unknown: The Definition of Aggression Revisited*, 17 MICH. ST. J. INT'L L. 377, 377–78 (2009). However, the definition was not binding on U.N. Member States and had no apparent impact on the Security Council. *Id*. at 378. Recently, the International Criminal Court ("ICC") was given jurisdiction over the undefined crime of aggression provided that the definition is consistent with the norms of the U.N. Charter. *Id*.

38. Sklerov, *supra* note 32, at 52–54.

39. *Id.* at 31. Information warfare creates serious problems in the distinction between use of force and mere coercion under Article 2(4). Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 84 (2001). Including all types of information warfare and cyberattacks would require an enormous expansion of Article 2(4). *Id*. Such an expansion would require international law to determine whether electronic incursions that may not necessarily create physical damage, but have significant economic and political effects, are substantial enough to constitute a use of force. *Id.* at 84–85. Professor Michael Schmitt proposed a framework that attempts to answer the question of whether cyberattacks constitute armed force or simply mere coercion. *Id*. at 85. Professor Schmitt believes we should evaluate the cyberattack using six criteria: severity, immediacy, indirectness, invasiveness, measurability, and presumptive legitimacy. *Id*.; *see also* Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 929–32 (1999). Once a cyberattack is determined to be an armed attack, the right to self-defense under Article 51 would be triggered. Barkham, *supra* note 39, at 85.

40. This scope of planning persisted since the drafting of the Charter. Yutaka Arai-Takahashi, *Shifting Boundaries of the Right of Self-Defence—Appraising the Impact of the September 11 Attacks on Jus Ad Bellum*, 36 INT'L LAW. 1081, 1087 (2002).

41. "Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition." Definition of Ag-

provides that aggression can only derive from a state.[42] Within the traditional *jus ad bellum* framework, the international community did not anticipate that nonstate actors would ascend to the level of a state capable of initiating an armed attack against another state.[43]

B. The Evolution of Attributing State Responsibility to Private Acts

Prior to the paradigm shift spurred by 9/11, states were not held legally responsible for the acts of nonstate or private actors.[44] Only acts by branches or entities of a state were held attributable to that state.[45] International law, however, did recognize the principle that a state can be bound by the actions of private persons, but only if those persons qualify as "agents" of the state.[46] International jurisprudence evolved to hold a state responsible for the acts of nonstate actors if the state exercised effective or overall control over the actors, then advanced to hold a state indirectly responsible if the state failed to prevent attacks from originating within its territory.

1. The "Effective Control" Test

In the *Nicaragua* case, the International Court of Justice ("ICJ") addressed whether the United States was responsible for the financing and support of contras operating in the Nicaragua-El Salvador conflict.[47]

---

gression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974).

42. Aria-Takahashi, *supra* note 36, at 1087.

43. *Id*. The law of armed force is governed by two bodies of law: *just ad bellum*, the law governing recourse to force, and *just in bello*, the law governing conduct of hostilities. Carsten Stahn, *Jus Post Bellum: Mapping the Discipline(s)*, 23 AM U. INT'L L. REV. 311, 311 (2008). Both principles are based in the moral justification for warfare and are intertwined with the just or unjust cause of recourse of force. *Id*. at 346.

44. Proulx, *supra* note 9, at 619.

45. *Id*. at 619–20.

46. *Id*. at 620. "Since the publication of Professor Bowett's Reprisals Involving Recourse to Armed Force, international courts have formally adopted this concept of attribution." *Id*.; *see also* D. Bowett, *Reprisals Involving Recourse to Armed Force*, 66 AM. J. INT'L L. 1 (1972).

47. René Värk, *State Responsibility for Private Armed Groups in the Context of Terrorism*, JURIDICA INT'L XI 184, 188 (2006), *available at* http://www.juridicainternational.eu/public/pdf/ji_2006_1_184.pdf. The U.S. consistently opposed Nicaragua's Sandinista government, a leftist political party with "close relations with the Soviet Union and Cuba," in Nicaragua. Davis B. Tyner, *Internationalization of War Crimes Prosecutions: Correcting the International Criminal Tribunal for the Former Yugoslavia's Folly in Tadic*, 18 FLA. J. INT'L L. 843, 850 (2006). The U.S. used various methods to undermine the regime, including cutting off aid, starting a trade embargo, and financing and supporting counter-revolutionary forces, including contras. *Id*. The

Even though it was clear that the rebels were a "proxy army" of the United States, and at times were "completely dependent on the United States' support,"[48] the ICJ refused to attribute responsibility to the United States.[49] The ICJ determined that:

> United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying or equipping of the contras, the selection of . . . targets, and the planning of the whole of its operation, is still insufficient in itself . . . for the purpose of attributing to the United States the acts committed by the contras . . . . For this conduct to give rise to legal personality of the United States, it would in principle have to be proved that the State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.[50]

In order to establish state responsibility under the Nicaragua decision, one must prove that state agents "participated in the planning, direction, support[,] and execution" of armed operations.[51] Thus, it became customary to analyze the level of effective control exercised by the agents of one state over the private actors of another state in order to determine the level of responsibility to attribute to the host-state.[52]

2. The "Overall Control" Test

Over a decade after the *Nicaragua* decision, the International Criminal Tribunal for the Former Yugoslavia ("ICTY") Appeals Chamber faced a similar issue in *Prosecutor v. Tadic*.[53] Tadic, a Bosnian Serb, participated in "ethnic cleansing" of Bosnian Muslims in 1992.[54] The issue in Tadic's appeal was whether "Bosnian Serbs constitute[d] a State" or whether

---

Nicaraguan government opposed the U.S. support of contras and argued that they were de facto agents of the U.S. *Id*.

48. Proulx, *supra* note 9, at 620.

49. Värk, *supra* note 47, at 188.

50. *Id*. (quoting Nicaragua, *supra* note 12).

51. Värk, *supra* note 47, at 189 (quoting Nicaragua, *supra* note 11).

52. Proulx, *supra* note 9, at 621.

53. *See* Prosecutor v. Tadic, Case No. IT-94-1-A, I.C.T.Y. App. Ch., at 49 (July 15, 1999).

54. Marco Sassoli & Laura M. Olson, *Prosecutro v. Tardic (Judgement)*, 94, 3 AM. J. INT'L L. 571, 571 (2000). Tadic was a former café owner who became involved in Serb Nationalism. Tyner, *supra* note 47, at 854. During the war in the Balkan Islands, Tadic reportedly ran a prison camp where he allegedly beat and murdered several prisoners. *Id*. The ICTY prosecuted Tadic as an agent of the state and convicted him of several offenses, including crimes against humanity and grave breaches of the Geneva Conventions. *Id*.

"[they] were organs or agents of the Federal Republic of Yugoslavia."[55] In rejecting the ICJ's effective control test, the Appeals Chamber ruled that overall control of a military organization is adequate to attribute state responsibility to "all acts of the organization."[56]

The *Tadic* court made an important distinction between military organized groups and non-military organized groups.[57] The former has a structure, chain of command, strict sets of rules to which members must conform, and is subject to the authority of the group's leader.[58] Thus to attribute responsibility to the host-state, the state would have to wield control of the group overall by equipping, financing, and coordinating or helping in the planning of its military activity.[59] For non-military groups, the threshold was even higher, requiring "specific instructions" to be delivered from the state to the group.[60]

The key difference between the *Nicaragua* and *Tadic* cases is degree of control—that is, the ICTY requires control beyond financing and equipping forces and should, but does not necessarily, include planning and supervision of military operations.[61] Importantly, the ICTY in *Tadic* focused on individual responsibility, distinguishing the case from *Nicaragua*, which focused on state responsibility.[62] After all, the *Tadic* court believed state responsibility should be based on a "realistic concept of responsibility."[63]

3. Other International Jurisprudence and the Shift towards Indirect Responsibility

Although *Nicaragua* and *Tadic* are the seminal cases evidencing the shift towards state responsibility over private action, other international jurisprudence can be instructional as well. *Nicaragua* and *Tadic* focus on the concept of direct responsibility—where a militarized group acts as an agent of the state or where the state retroactively endorses the act.[64] The

---

55. Sassoli & Olson, *supra* note 54, at 572. The issue in *Tadic* was whether international human rights law applied, not state responsibility. James Crawford, *Human Rights and State Responsibility* 1, 5 (12th Raymond & Beverly Sackler Distinguished Lecture Series, Univ. of Conn., 2009).

56. Sassoli & Olson, *supra* note 54, at 572.

57. Proulx, *supra* note 9, at 621.

58. *Id*.

59. *Id*.

60. *Id*. Alternatively, the non-military group standard could be met if the host-state approved of or endorsed the act ex post facto. *Id*. at 621–22.

61. Värk, *supra* note 47, at 189.

62. Crawford, *supra* note 55, at 5.

63. Värk, *supra* note 47, at 189 (internal quotation marks omitted).

64. Proulx, *supra* note 9, at 624.

issue becomes more complicated when there is no causal link between the host-state and the actor—where states have no knowledge or control over organizations within their boundaries.[65] The only link between the two entities is that they both happen to operate in the same territory.[66]

1923's *Tellini* incident foreshadowed the trend away from the traditional *jus ad bellum* framework towards the notion of indirect state responsibility for internal private actors.[67] While overseeing the delineation of the Greek-Albanian border, several members of an international commission were assassinated on Greek territory.[68] Although the League of Nations did not hold Greece legally responsible for the assassination,[69] it opined that "responsibility of a State is only involved by the commission in its territory of a political crime against . . . foreigners if the State has neglected to take all reasonable measures for the prevention of the crime and the pursuit, arrest and bringing to justice of the criminal."[70]

United States v. Iran (the "Tehran Hostages Case") takes the concept of *Tellini* and indirect state responsibility one step further.[71] In 1979, a militant group attacked a U.S. Embassy in Tehran, Iran. Despite several requests for help, no Iranian forces intervened.[72] The Embassy was eventually invaded and the consular, staff, and visitors were taken hostage.[73] Somewhat foreshadowing *Tadic*, the ICJ asked whether "the militants acted on behalf of the State, having been charged by [an] organ of the Iranian State to carry out a specific operation."[74] Finding no direct involvement, the ICJ then considered indirect involvement.[75] The Court believed "the Iranian Government failed altogether to take any 'appropriate steps' to protect the premises, staff and archives of the United States' mission against attack by the militants, and to take any steps either to prevent this attack or to stop it before it reached its completion."[76]

---

65. *Id*. at 624, 627.

66. *Id*. at 627.

67. *Id*. Following the assassination, the League of Nations formed a special committee to address the legal matters raised by the incident.

68. Crawford, *supra* note 55, at 4.

69. Proulx, *supra* note 9, at 627.

70. Crawford, *supra* note 55, at 4 (internal citation omitted).

71. *See* Tehran Hostages Case (U.S. v. Iran), 1980 I.C.J. 64 (May 24) [hereinafter Tehran].

72. Leo Gross, *The Case Concerning United States Diplomatic and Consular Staff in Tehran: Phase of Provisional Measures*, 74, 2 AM. J. INT'L L. 395, 395 (1980).

73. *Id*.

74. Proulx, *supra* note 9, at 627.

75. *Id*. at 627–28.

76. *Id*. at 628 (quoting Tehran).

The *Tehran* decision drew a clear boundary between direct responsibility and indirect responsibility.[77]

4. United Nations Security Council Resolution 1373

The events of 9/11 served as a pivotal point in the development of contemporary indirect state responsibility.[78] International law would not support a military reprisal in Afghanistan solely against al Qaeda, as the terrorist group was not the same as a state.[79] The United States "sought to impute al Qaeda's conduct to Afghanistan simply because the Taliban had harbored and supported the group."[80] After the events of 9/11, the United States seemingly eliminated the distinction between direct and indirect state responsibility.[81]

More than two weeks after 9/11, the U.N. Security Council adopted Resolution 1373.[82] The resolution provides that "all States shall . . . [r]efrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, . . . prevent the commission of terrorist acts, . . . [and] deny safe haven to those who . . . support[] or commit terrorist acts."[83] The United States made a case against the Tali-

77. Proulx, *supra* note 9, at 628. After the decision, it became clear that the initial focus of the direct responsibility standard hinges on the individuals or groups involved instead of the actions of the host-state. *Id*. The objective became establishing whether the unlawful act or omission of the person or group was directly attributable to the state. *Id*.

78. *Id*. at 634. On September 11, 2001, nineteen terrorists hijacked four commercial aircrafts, flew two into the World Trade Center, one into the Pentagon, and the last crashed in a Pennsylvania field. Sean D. Murphy, *Terrorist Attacks on World Trade Center and Pentagon*, 96 AM. J. INT'L L. 237, 237 (2002). Approximately three thousand people were killed in the incidents, the worst casualties the U.S. has experienced in a single day since the American Civil War. *Id*. After the attacks, the U.S. suspected that the hijackers were funded by a Saudi Arabian expatriate, Osama Bin Laden, and based in Afghanistan working through his terrorist network, al Qaeda. *Id*. at 238.

79. Proulx, *supra* note 9, at 635.

80. Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHI. J. INT'L L. 83, 89 (2003).

81. Proulx, *supra* note 9, at 636; *see also* TAL BECKER, TERRORISM AND THE STATE; RETHINKING THE RULES OF STATE RESPONSIBILITY 218 (2006) ("Operation Enduring Freedom was explicitly justified on the contentious claim that the act of harbouring terrorists is legally indistinguishable from the actual perpetration of terrorist acts.").

82. Michael Wood, *The Law on the Use of Force: Current Challenges*, 11 SYBIL 1, 6 (2007); *see also* S.C. Res. 1373, U.N. SCOR, 4385th Mtg., U.N. Doc. S/RES/1373 (Sept. 28, 2001).

83. S.C. Res. 1373, U.N. SCOR, 4385th mtg., U.N. Doc. S/RES/1373 (2001). For more implications of Resolution 1373 and cyberwarfare, see Toby L. Friesen, *Resolving Tomorrow's Conflicts Today: How New Developments Within the U.N. Security Council can be Used to Combat Cyberwarfare*, 58 NAVAL. L. REV. 89 (2009); *see also* Sumon Dantiki, *Power Through Process: An Administrative Law Framework For United Na-*

ban, claiming that it failed to prevent a terrorist attack that originated within its boundaries and harbored al Qaeda members.[84] Both the resolution and U.S. practice reinforced the international community's new commitment to fighting terrorism.[85] As a result, the indirect responsibility standard has become the prevailing view in the area of attribution.[86]

II. ATTRIBUTION—GETTING IT RIGHT IN THE SELF-DEFENSE ANALYSIS IS OF EXTREME IMPORTANCE

This section examines why attribution is a necessary part of the Article 51 right of self-defense analysis, despite the inherent difficulties of online attribution. Once an attack, online or kinetic, qualifies as an armed attack, it seemingly gives the injured state the right to act in self-defense. The issue of attributing responsibility of private actors to a state is a complex issue within the realm of kinetic terrorism, but the nuances of the doctrine become even more pronounced when an attack is strictly electronic.

The relatively new standard of imputing state responsibility over private actors imposes a greater amount of force on states' affirmative duty to prevent their territory from becoming attackers' sanctuaries.[87] Traditionally, states were obligated to use due diligence to prevent criminal acts within their territories directed at other nations.[88] However, after the events of 9/11 and the imposition of obligations within Resolution 1373, states have a continual duty to prevent terrorist attacks from originating

---

tions Legislative Resolutions, 40 GEO. J. INT'L L. 655, 655 (2009) (arguing that Resolution 1373 created a binding obligation on states to reform domestic law in order to more effectively fight international terrorism). Under Article 39 of the U.N. Charter, the Security Council can impose binding resolutions on member states if necessary to maintain peace and security. Peter Hulsroj, *The Legal Function of the Security Council*, 1 CHINESE J. INT'L L. 59, 60 (2002). *But see* Lorraine Finlay, *Between a Rock and a Hard Place: The Kadi Decision and Judicial Review of Security Council Resolutions*, 18 TUL. J. INT'L & COMP. L. 477 (2010) (discussing the implications of Security Council resolutions being subject to judicial review).

84. Proulx, *supra* note 9, at 638.

85. *Id*. at 637–38.

86. *Id*. at 638. On Sept. 12, 2001, the Security Council adopted Resolution 1368 (2001) recognizing "the inherent right of individual and collective self-defence in accordance with the Charter." Wood, *supra* note 82, at 6. More than two weeks later, the Security Council adopted Resolution 1373 (2001), which again reaffirmed "the inherent right of individual and collective self-defence as recognized by the Charter of the United Nations." *Id*.

87. Graham, *supra* note 35, at 90.

88. Sklerov, *supra* note 32, at 42 (citing *In re* S.S. Lotus, 1927 P.C.I.J. (ser. A) No. 10, 4, 88 (Moore, J., dissenting)).

within their respective national boundaries.[89] Thus, a state that has the ability to prevent attacks and fails to do so ultimately fails to fulfill its duty.[90]

In his 1995 article, Vincent-Joël Proulx advocates doing away with the trans-substantive rule of attribution and shifting the entire model towards strict liability.[91] Proulx supports his argument largely on the basis international community's intent on eliminating terrorism, the Security Council's condemnation of terrorism, and its determination to "eliminate threats to peace and security 'by all necessary means.'"[92] Proulx also argues that because the evidentiary standards required for attribution present insurmountable barriers for injured states, strict liability should be imposed on states that either did not or could not prevent a terrorist attack from emanating within its borders.[93] As such, Proulx believes that circumventing the rule of attribution better serves the international com-

---

89. Graham, *supra* note 35, at 93. The duty generally consists of: (1) the enactment of laws criminalizing international cyber attacks from within the national territory, (2) conducting thorough investigations into cyberattacks, (3) prosecuting those who have participated in international cyberattacks, and (4) cooperating with victim-states' investigations and prosecutions of those involved. *Id*. at 93–94.

90. Sklerov, *supra* note 32, at 43 (internal citations omitted).

91. Proulx, *supra* note 9, at 643–56. It should be noted that Proulx's theory of state strict liability does not impose immediate absolute liability. *Id*. at 656. In order to avoid abuse of weaker states, that is, developing countries that may not have the capabilities to combat terrorism, Proulx would implement a two-tiered strict liability system. *Id*. Once responsibility has been established on the host-state and the focus has shifted onto it, the state will have an opportunity to prove how it has exhausted all available means to thwart the terrorist attack. *Id*. at 657.

92. *Id*. at 643; *see also* Rob McLaughlin, *The Legal Regime Applicable to Use of Lethal Force When Operating Under a United Nations Security Council Chapter VII Mandate Authorising 'All Necessary Means'*, 12 J. CONFLICT & SECURITY L. 389 (2007) (examining the use of lethal force under an "all necessary means" resolution). It is important to note that Proulx's argument of circumventing attribution is largely grounded in policy. He does not discuss the practical difficulties associated with circumventing the rule. He does, however, analogize his theory of state strict liability to the domestic U.S. law of products liability. Proulx, *supra* note 9, at 652–54. Within domestic products liability, manufacturers are often found strictly liable because public policy requires that manufacturers be held accountable for their products' quality. *Id*. at 653 (citing Escola v. Coca Cola Bottling Company, 150 P.2d 436 (Cal. 1944)). Referring to a state's duty to prevent, Proulx believes that governments are in a better position to thwart terrorist attacks from originating within their territory, just as manufacturers are more aware of potentially hazardous products than the unwary consumer. Proulx, *supra* note 9, at 653. "As with the Coke bottle manufacturer who has exclusive knowledge over the manufacturing process, the host-state is better positioned than the injured state to know, for example, what logistical, intelligence, police, and military means are at its disposal to eliminate the threat." *Id*. at 655.

93. *Id*. at 643–57.

munity's interest in eradicating terrorism.[94] While potential effectiveness of circumventing attribution is not the focus of this Note, it is clear that such a method is untenable within the rapidly growing realm of cyberattacks and cyberterrorism.

A. Attribution in the Cyberattack Context

Although states are under a continual, affirmative obligation to prevent attacks from emanating from within their territory, the effectiveness of prevention is limited as cyberattacks are extremely difficult to prevent.[95] Attribution of an attack and characterizing the type of attack are imperative in the context of cyberattacks.[96] Fundamentally, attribution ensures that an injured state responding in self-defense does not target innocent people or states.[97] Attribution also plays a critical role in determining the nature and character of an attack, which is the first step in developing a lawful response, whether offensive or defensive.[98] Attribution in the online context involves two issues: "attacker-attribution"—who is responsible for an attack—and "attack-attribution"—characterizing what kind of attack it was.[99]

B. Attacker-Attribution: "Who Dun It?"

Identifying an online attacker is problematic because the methods we use to identify kinetic attackers implicitly assume physically-based activity in the tangible world.[100] Cyberattacks do not take place in the tangible world, and as such, they do not display the characteristics common to

---

94. *Id*. at 643. Although outside the scope of this Note, it is interesting to note that in his discussion of the strict liability model, it appears that Proulx appears to easily dismiss the notion of infringing upon state sovereignty. *Id*. at 658–59. Proulx states that it is "desirable and more efficient" to sacrifice some sovereignty than fail to prevent widespread death and terror. *Id*. at 659. For further discussion of the state sovereignty in the information age, see Adeno Addis, *The Thin State in Thick Globalism: Sovereignty in the Information Age*, 37 VAND. J. TRANSNAT'L L. 1 (2004); Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009). "Despite the importance of state sovereignty, governments in the nineteenth century began to see the benefits of sacrificing some sovereignty in exchange for increased predictability." Jensen, *supra* note 25, at 214 (internal citation omitted).

95. Barkham, *supra* note 39, at 83; *see also supra* Part I.B.4.

96. Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 414 (2007).

97. *Id*.

98. Brenner, *Attribution and Response*, *supra* note 9, at 405.

99. *Id*.

100. *Id*. at 409.

their physical counterparts.[101] In the physical world, determining attacker liability often turns on a "place" where an attack emanated from or occurred.[102] Places, however, tend to be much less conclusive in the context of cyberattacks and online attribution.[103]

Determinations of attack origin are less conclusive in cyberattacks because the server location of an attack does not likely reflect the true location of origin.[104] Cyberattackers commonly use "stepping stones"—computers used by the cyberattacker but owned by ignorant parties—in their attacks.[105] While these stepping stones can be physically located anywhere in the world, their physical location is irrelevant in cyberspace.[106] For example, the use of Chinese servers in a cyberattack could mean the attacks originated in China, or that the attackers were located in Russia, Brazil, Pakistan, or anywhere else in the world and deliberately used Chinese servers to mask the true origination point of the attack.[107] Until investigators can reliably establish attack origination in real-space,

---

101. *Id*. In the physical world, attacker-attribution is far less problematic. *Id*. at 406. In warfare, military attackers often wear distinct uniforms indicating their national affiliation and speak the language of their country of origin. *Id*. Criminal investigations often focus on finding evidence at a physical crime scene. *Id*. at 407. For example, witnesses may be able to identify the attacker and physical evidence, like DNA, can be traced to a particular individual. *Id*. This method assumes that the attacker or perpetrator was, and still is, physically located in the geographical area. *Id*. Terrorism occupies some middle ground in between warfare and criminal investigations, with regard to attacker-attribution. *Id*. Terrorists often identify themselves as representatives of a particular group, generally so the group can take credit for the attack. *Id*. at 408; *see also* KIM CRAGIN & SARA A. DALY, THE DYNAMIC TERRORIST THREAT, 37–38 (2004) (explaining that the Real Irish Republican Army and Hamas generally take credit for attacks, while the Revolutionary Armed Forces of Columbia and al Qaeda do not). Sponsoring terrorist groups often take credit for attacks in messages online or on videotapes delivered to the media. Brenner, *Attribution and Response*, *supra* note 9, at 408. In addition, terrorist attacks may be attributed to a particular group based on the structure and style of the attack. *Id*.

102. Brenner, *Attribution and Response*, *supra* note 9, at 409.

103. *Id*.

104. *Id*.

105. *Id*. The concept of geographical places is further distorted by "packet switching," in which packets of data travel the shortest electronic route to their destination. Condron, *supra* note 96, at 409. The shortest electronic route, however, does not necessarily correspond to the shortest geographical route. *Id*. Data transfer relies on "existing network traffic loads," and therefore "shortest" corresponds more to time than geographic distance. *Id*.

106. Brenner, *Attribution and Response*, *supra* note 9, at 409.

107. *Id*. at 409–10; *see, e.g.*, Nathan Thornburgh, *The Invasion of the Chinese Cyberspies*, TIME, Sept. 5, 2005, at 34, 34 ("In the world of cyberspying, locating the attackers' country of origin is rare. China, in particular, is known for having poorly defended servers that outsiders from around the world commandeer as their unwitting launchpads.").

attacker-attribution is predicated on mere inferences.[108] Even if cyberattacks are repeated over long periods of time, attacker-attribution would still have to be drawn from inferences of what would appear to be the same point of origin.[109]

Relying on inferences to identify the point of origin in cyberattacks introduces an element of ambiguity into the response calculus.[110] Further, an identified cyberattack origination point may be inconclusive, as essentially anyone has the ability to launch an anonymous transnational cyberattack.[111] At most, inferential data regarding point of attack origin serve merely as clues to attacker-attribution.[112] Cyberspace eliminates law enforcement's default assumption that an attacker is insular.[113] It breaks a crime scene into debris, making it extremely difficult to identify the point of attack origin and link it to the attacker.[114] At the very least, it may re-

---

108. Brenner, *Attribution and Response*, *supra* note 9, at 410; *see also* Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CARNEGIE MELLON SOFTWARE ENGINEERING INST. (Nov., 2002), www.cert.org/archive/pdf/02sr009.pdf (discussing that the Internet was neither designed for tracking and tracing users nor designed to resist untrustworthy users, and how today's high-threat environment far exceeds the Internet's design parameters).

109. Brenner, *Attribution and Response*, *supra* note 9, at 410; *see, e.g.,* Eric Filiol, *Operational Aspects of Cyberwarfare or Cyber-Terrorist Attacks: What a Truly Devastating Attack Could Do*, ESIEA—OPERATIONAL VIROLOGY & CRYPTOLOGY LABORATORY (2009), http://www.esiea-recherche.eu/data/eciw09.pdf (discussing the main characteristics of a cyberattack: "not only the true origin of the attack must remain hidden, but also must be possible to wrongly frame an innocent party (another country or group) as the perpetrator of the attack (fooling the digital evidence). From a military perspective, the main interest is to avoid or to delay the target reaction by misleading it.").

110. Brenner, *Attribution and Response*, *supra* note 9, at 412.

111. *Id*.

112. *Id*. at 414. However, as terrorism migrates online, the point of origin may gain more importance in attacker-attribution. For example, in 1994, employees at the Rome Air Development Center, the U.S. Air Force's R&D facility in upstate New York, discovered that their computer systems had been hacked. *Id*. The Air Force, Secret Service, and FBI found that the attackers routed their attacks through several computers in multiple countries. *Id*. at 414–15. With the assistance of Scotland Yard, the investigators identified two adolescents as the attackers. *Id*. at 415; *see also* RICHARD POWER, TANGLED WEB: TALES OF DIGITAL CRIME FROM THE SHADOWS OF CYBERSPACE 65–75 (2000) (detailing the events of the Rome Labs scenario and what led to the capture of the teen cyberattackers—Datastream Cowboy and Kuji).

113. Brenner, *Attribution and Response*, *supra* note 9, at 415. In real-space crime and terrorism, a localized crime scene becomes the focus of the investigation. *Id.* at 417. Evidence, witnesses, and connections give the scene a comprehensible focus and make it a manageable task. *Id*. In cyberspace, however, anyone can anonymously launch an attack from any point connected to the Internet and repeat the attacks with a frequency not possible in the real-world. *Id*. at 418.

114. *Id*.

sult in false positives, leading the investigators to assume that an intermediary stepping stone is the originating point of a cyberattack.[115]

The issue of attacker-attribution remains the same even if the origination point is traced back to a state that sponsors terrorism.[116] A point of attack origin located in terrorist state would still be inconclusive—the state may or may not have participated in the attack.[117] On the other hand, the fact that a cyberattack does not originate from a terrorist state does not mean that the state was not involved in the attack.[118] While it may be tempting, perhaps even convenient, to implicate a terrorist state from the mere appearance that it launched a cyberattack, they are no exception to the lack of clarity in attacker-attribution.

Ultimately, the mere fact that an extraterritorial cyberattack appears to have been launched from a particular state cannot support the conclusion that either state or nonstate actors launched the attack from within that state.[119] The physical limitations of the real world make it reasonable to draw inferences to link an attack to an attacker.[120] The absence of those limitations on the Internet makes it exceedingly difficult to predicate similar inferences to a cyberattack.[121] As such, any inferences made from the point of attack origin or from the victim-state cannot sustain a conclusion of direct or indirect state responsibility.[122]

C. Attack-Attribution: "What Is It?"

Determining the identity of a cyberattacker or cyberterrorist will likely be closely associated with determining the nature of an attack, or "attack-

---

115. *Id*. This could have happened in the Rome Labs example. *Id*. Investigators originally tracked the hackers to an ISP in New York City and to a group of hackers whose members were convicted of unlawful intrusion crimes in years earlier. *Id*. Given their geographical connection to the hackers, it would have been logical for the investigators to assume that the ISP was the point of attack origin. *Id*. at 418–19. In addition, it is important to note that the investigators were unable to track the hackers back to the point of attack origin through online or electronic means. *Id*. at 419. They did it the old fashioned way—with informants. *Id*.

116. *Id*. at 423.

117. *Id*.

118. *Id*.

119. *Id.* at 427.

120. *Id*. at 428. For example, an attacker gaining entry to a house protected by an alarm system by using the correct alarm code suggests that the attacker knew the victim. *Id.* A burgled jewelry store or bank with an uncompromised safe suggests that the perpetrator was an employee, former employee, or someone who the employee shared the safe's code with. *Id*. In both cases, investigators can infer with a high degree of certainty as to who performed the attack and where. *Id*.

121. *Id*.

122. *Id*. at 429.

attribution."[123] Like attacker-attribution, online attack-attribution is inherently more problematic than real-world attack-attribution.[124] However, identifying the nature or character of a cyberattack is the first step in evaluating whether it qualifies as an armed attack under Article 51 and ensuring that any response functions within the limitations of necessity and proportionality.[125] The overarching problem with online attack-attribution is that it is difficult to determine the nature of the attack because the indicators we must rely on—point of attack origin, point of occurrence, and motive—develop an inherent ambiguity not present in the real-world.[126] This is because cyberspace makes it possible for anyone with an Internet connection to launch an attack on another computer in another country.[127]

A response strategy is predicated on the premise that a state can know, or quickly determine, what kind of attack it was subject to and what is needed to neutralize the attackers.[128] This is complicated by states' general allocation of response authority for crime and terrorism to law en-

123. *Id*.

124. *Id*. at 433–34. According to Professor Brenner, real-world attacks fall into two categories: crime/terrorism and warfare. *Id*. at 431. Crime usually involves civilians inflicting certain types of harm on each other—for example, murder, rape, assault, fraud—and is generally limited in scale due to the constraints of physical reality. *Id*. For example, a mugger robs one victim, a rapist assaults one victim, a murder kills one person; in each case, the victimization is limited. *Id*. at 432. Although terrorism is considered a crime, it is distinguished from crime in that it seems irrational, in that it lacks obvious motive, and the scale with which it is committed is much larger than crime. *Id*. at 431. For example, the World Trade Center attacks were irrational in that they did not result in financial gain or redress personal grievances. *Id*. Terrorism does not develop from personal matters, but from ideology. *Id*. at 432. Futhermore, terrorists differ from criminals in that terrorists aim to cause as much death and injury as possible. *Id*. The harm inflicted by a terrorist will almost certainly surpass harm attributable to any individual crime, as terrorists often inflict generalized harm. *Id*. at 432–33. Real-world warfare is generally easier than crime or terrorism to identify. *Id*. at 433. A state's military launching an attack on another state's territory indicates that we have entered the theater of war. *Id*.

125. Graham, *supra* note 35, at 100–01 ("[A] state may lawfully resort to force when acting in self-defense against an armed attack, provided it conforms to the customary international law concepts of necessity and proportionality.").

126. Brenner, *Attribution and Response*, *supra* note 9, at 435. For example, figuring out where an attack was launched from in the physical world is much more conclusive. *Id*. The fact that a victim-state believes a cyberattack was launched from a particular state is a consideration, but it carries much less weight online than it does in the physical world. *Id*.

127. *Id*.

128. *Id*. at 436.

forcement and warfare to the military.[129] One issue this separation presents is that the response process may be delayed while respective decision-makers attempt to determine the nature of a cyberattack.[130] Decision-makers may also misunderstand the nature of an attack.[131]

The real-world indicators we rely on to determine the nature of an attack—point of attack origin, point of occurrence, and motive for an attack—are often lacking or unreliable in cyberattacks.[132] Motive is a particularly distinguishing factor for cyberattacks.[133] The problem arises with a state's ability to determine the motive behind a particular attack,[134] and becomes especially challenging when no obvious motive exists.[135]

---

129. *Id*. This distribution of responsibility is generally carefully adhered to: "[c]ivilian law enforcement does not respond to war and the military does not respond to crime." *Id*.

130. *Id*.

131. *Id*. Misunderstanding the nature of a cyberattack stems from both partitioned responsibility and because we generally assume that crime is a "localized phenomenon." *Id*. at 437. For example, a cyberattack targeting a corporate computer system may be inferred to be cybercrime, as we tend to assume that criminals target civilians. *Id*. at 436. This conclusion would further be supported if the attackers' behavior conformed to what we expect to be criminal—extracting funds or personal information from corporate databases—and, as such, would likely be responded to by civilian law enforcement. *Id*. Those inferences, however, could be wrong. The attack could just as easily be cyberwarfare. *Id*. at 437. For example, China's warfare strategy specifically focuses on attacking civilian entities, including financial entities and infrastructure. *Id*.; *see also* U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 109th Cong. (2006), *available at* http://www.uscc.gov/annual_report/2006/annual_report_full_06.pdf ("China is actively improving its non-traditional military capabilities . . . . China's approach to exploiting the technological vulnerabilities of adversaries extends beyond destroying or crippling military targets. Chinese military writings refer to attacking key civilian targets such as financial systems."). Indeed, if we continue with the "civilian-attacks-are-crime" misinterpretation, we may begin to see serious consequences resulting from damage to financial systems or infrastructure. Brenner, *Attribution and Response*, *supra* note 9, at 437. The same could be said of cyberterrorism and cyberwarfare. *Id*. Cyberterrorist attacks usually occur as a sequence of attacks which may be spatially and temporally separated. *Id*. As a result, law enforcement may not consider that each attack is part of a larger, broader attack. *Id.* Thus, a response would likely be uncoordinated and isolated, with officers in various locations responding differently to a large, singular threat. *Id*.

132. *Id*. at 437–38. As seen above, the importance of point of origination and point of occurrence generally erode as attacks are launched online. *Id*. at 438.

133. *Id*. For example, profit is a likely motive for most cybercrime, ideology for cyberterrorism, and state enmity for cyberwarfare. *Id*.

134. *Id*. An example of this is the Titan Rain and Moonlight Maze cyberattacks. *Id*. Titan Rain is the U.S. government's designation for a series of coordinated cyberattacks on American systems from 2003 to 2005. Thornburgh, *supra* note 107. The attacks were tracked back to routers in China, but the identity of the hackers was never discovered. *Id*. The hackers gained access to several sensitive U.S. networks including those at Lockheed Martin, NASA, Redstone National, and Sandia National Laboratories. *Id*. Moonlight Maze refers to a 1998 "incident in which U.S. officials accidentally discovered a pattern

The scenario in which we will be unable to determine if a cyberattack is a mere crime, a terrorist attack, or warfare presents the greatest challenges for the current response model under Article 51, and therefore presents the greatest risks of unlawful retaliation for the injured state.[136] Countries that partition response authority between civilian law enforcement and military agencies, like the United States,[137] are particularly vulnerable to these risks.[138] If responders cannot determine what kind of

---

of probing of computer systems at the Pentagon, NASA, Energy Department, private universities, and research labs . . . ." *Cyberwar!*, PBS.ORG, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/ (last visited Mar. 1, 2011). The cyberattack was traced back to the Soviet Union but the identity of the attackers was never discovered. *Id*. In both Titan Rain and Moonlight Maze we know what the attackers did, but have not determined why they did it. Brenner, *Attribution and Response*, *supra* note 9, at 438.

135. Brenner, *Attribution and Response*, *supra* note 9, at 439. The motives behind most cybercrime attacks are usually apparent—profit or revenge. *Id*. at 438. Cyberterrorists, however, in an effort to fund their real-world kinetic attacks have introduced us to "mixed motive" scenarios: where the motive for a cybercrime is to profit, but the motive for achieving financing is to engage in terrorism. *Id*. This scenario has very few implications in the development of a response and attack-attribution because civilian law enforcement is responsible for both crime and terrorism. *Id*.

136. *Id*. at 439.

137. Several federal U.S. statutes prohibit the comingling of partitioned authority. *See* Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA Patriot Act*, 88 TEX. L. REV. 1795, 1797–98 (2010). For example, the National Security Act of 1947 prohibits the CIA from employing "police, subpoena, or law enforcement powers" or engaging in "internal security functions." *Id*. at 1797 (citing 50 U.S.C. § 403–4a(d)(1) (2006)). The Posse Comitatus Act of 1878 generally criminalizes using the military for law enforcement functions. *Id*. at 1797–98 (citing 18 U.S.C. § 1385 (2006)). The 1878 Act even reflects the idea that the military must remain subordinate to civilian law enforcement. *Id*. at 1798. In addition, the Privacy Act of 1974 promotes freedom from government inspection and the ability to monitor information about oneself. *Id*. However, a narrow reading of the Act could even prevent federal civilian law enforcement agencies from cooperating. *Id*.

138. Brenner, *Attribution and Response*, *supra* note 9, at 439. This discussion is implicitly based on the United States' current response authority model. *Id*. at n.277. This author is most familiar with the U.S. response model, which is considered the most extreme model of partitioned response responsibility. *Id*. Response authority between law enforcement and the military is not as rigidly divided in some other countries. *Id*.; *see also* DONALD E. SCHULZ, THE UNITED STATES AND LATIN AMERICA: SHAPING AN ELUSIVE FUTURE 37 (2000) ("As matters now stand, many governments feel they have no choice but to bring the armed forces into law enforcement. The alternative is rampant criminality and national insecurity."). *But see* DANIELLA ASHKENAZY, THE MILITARY IN THE SERVICE OF SOCIETY AND DEMOCRACY: THE CHALLENGE OF THE DUAL-ROLE MILITARY 5 (Daniella Ashkenazy ed., 1994) ("[T]he military in democratic societies ha[s] not been assigned a role as a domestic law enforcement agency, with the exception of extreme circumstances of insurrection or collapse of domestic public order beyond the capabilities of civilian

cyberattack occurred or the severity of the effects,[139] they may not be able to correctly assume or assign responsibility to respond.[140] This leaves open the possibility that no response will result.[141]

Ultimately, the United States and countries with similarly segmented response models could be targets of cyberterrorism or cyberwarfare, potentially facing dispersed attacks. Such nations may not realize the nature of the attacks until extensive damage has incurred.[142] Local law enforcement would likely focus on each separate, seemingly localized attack, without appreciating the attack's role as a small part of a larger attack.[143] The possibility that the United States and similar countries could be subject to erratic and concerted cyberattacks by one or more organized groups of nonstate actors is all too real.[144] While the damage and loss of

---

police . . . ."). While militaries take on different roles at various times as perceived threats change, armed forces in democracies are often defensive by nature. *Id*.

139. *See, e.g.*, Barkham, *supra* note 39, at 84–93 (discussing cyberattacks and the distinction between use of force under Article 2(4) and mere coercion).

140. Brenner, *Attribution and Response*, *supra* note 9, at 439. An example of this would be a scenario in which intermittent, small-scale cyberattacks exploit the gap between Articles 2(4) and 51. Barkham, *supra* note 39, at 83. For instance, consider a scenario in which cyberattackers launched small-scale attacks in New York, Los Angeles, Chicago, and Las Vegas. If the effects of the attacks were noticed, local law enforcement would respond to each individual attack. The cyberattacks might appear as separate, uncoordinated attacks and each individual local law enforcement agency might not share information or coordinate their responses. Local law enforcement would deal discretely with each separate attack, unaware that they were responding to part of a larger attack. Brenner, *Attribution and Response*, *supra* note 9, at 439–40. Thus, where the intermittent, small-scale cyberattacks might be sufficient to constitute an armed attack if viewed in the aggregate, because of partitioned response responsibility, larger-scale Article 51 response would not result. *Id*.

141. *Id.*; *see also* Jill R. Aitoro, *Simulation Shows Government Lacks Policies Needed to Respond to Cyberattack*, NEXTGOV.COM (Feb. 16, 2010), http://www.nextgov.com/nextgov/ng_20100216_5378.php (simulation of a cyberattack against the U.S.'s critical infrastructure demonstrated how the cascading effects can cripple networks and illustrated the government's difficulty in responding). "As bandwidth was overwhelmed, millions of infected cell phones were shut down, the Internet slowed to a crawl and portions of the electric grid shut down as cyberattackers targeted a fictitious Web application electric utilities use to exchange bulk power service according to demand. Transportation systems, the Stock Exchange and financial institutions were also affected as networks failed." *Id*. Panelist discussions included whether the federal government could declare the cyberattack an act of war, whether the president's administration would be forced to respond by imposing martial law, and demanding that other countries cooperate with investigations. *Id*.

142. Brenner, *Attribution and Response, supra* note 9, at 439.

143. *Id*. at 439–40; *see* Arquilla, *supra* note 2 (fictional, but realistic, scenario of the world's first cyberwar launched by anonymous nonstate actors).

144. Brenner, *Attribution and Response*, *supra* note 9, at 440.

life might not be as immediate as kinetic terrorism on a 9/11 scale, cyberattacks of these sort could be just as, if not more, devastating, especially if recurring.[145]

The possibility of concerted cyberattacks by nonstate actors highlights the problem with states' segmented internal response authority in attack-attribution.[146] Civilian law enforcement and military personnel are extremely limited in their ability to collaborate in responding to attacks.[147] States assume they will be able to maintain internal order with civilian law enforcement and external stability with the military.[148] We have seen, however, that cyberspace erodes the validity of our real-world assumptions.[149]

D. Attribution Matters

Admittedly, determining attacker- and attack-attribution for cyberattack is a very difficult task.[150] While prevention is permitted, its effectiveness is limited.[151] Even with increased computer security, there is little that a potential target can do to stop an assault coming in from beyond its borders.[152] Nonetheless, the United States and other U.N. Member States have a continuing obligation to abide by the U.N. Charter with "entire good faith and scrupulous care."[153] This allows victim-states to retaliate only against states that have breached Article 2(4) by either directly attacking the victim-state, exercising control over nonstate actors

---

145. *Id*.

146. *Id*.

147. *Id*. Professor Brenner attributes this to the "persistence of the internal-external threat dichotomy." *Id*. at 440. Historically, rules that are designed to maintain internal order have not been implicated in a state's efforts to resist external threats. Brenner, *Toward a Criminal Law*, *supra* note 1, at 45. Internal rules are simply not applicable to the character and source of the outside threats. *Id*. Such rules are significant as they determine how a state will be able to use its resources on an external threat. *Id*. If a state is experiencing internal disorder and devastation, it will likely be unable to focus such resources on fighting external threats. *Id*.

148. Brenner, *Attribution and Response*, *supra* note 9, at 440; Brenner, *Toward a Criminal Law*, *supra* note 1, at 65–76.

149. Brenner, *Attribution and Response*, *supra* note 9, at 440. Physical proximity and environment constraints, scale or number of "crimes" a person can commit in a given period, and patterns of crime in the real-world are not applicable in cyberspace. Brenner, *Toward a Criminal Law*, *supra* note 1, at 65–75.

150. Christopher E. Lentz, *A State's Duty to Prevent and Respond to Cyberterrorist Acts*, 10 CHI. J. INT'L L. 799, 813–16 (2010) (discussing "[a]ttribution and [i]ts [i]mpossibly [h]igh [h]urdle").

151. Barkham, *supra* note 39, at 83.

152. *Id*. at 83–84.

153. John R. Kennel, 48 C.J.S. *International Law* § 63 (2010).

that have attacked the victim-state, or breaching their duty to prevent nonstate actors from launching attacks within their territory.[154] It also requires that states limit their responses to fit within the principles of necessity and proportionality.[155]

While some types of cyberattacks will fit easily within the structure of Articles 2(4) and 51,[156] evaluating whether localized but widespread cyberattacks trigger the right to self-defense depends on the attacks' effects and frequency.[157] Allowing states to respond without determining attacker- or attack-attribution might permit acts that would weaken the U.N. Charter's prohibition on the use of force.[158] Circumventing the rule of attribution would allow beleaguered states too much autonomy in determining the scope and intensity of an appropriate response.[159] Such practice would surely erode Article 51's purpose of limiting the frequency and scale of forceful self-defense to those rare times where it would be appropriate.[160]

This applies with particular force to cyberattacks as the scope of the attack and the identity of the attacker are usually unknown or uncertain. In the context of Article 51 self-defense, uncertainty is troublesome. Unless a victim-state is able to conclusively determine attacker-attribution—that is, which state is liable for failing to prevent an attack from being launched within its territory—it may very well retaliate against an innocent state, resulting in unwarranted death and destruction.[161] Furthermore, unless a state has fully determined the damage and effects inflicted

---

154. *See* discussion *infra* Part I.

155. Jensen, *supra* note 25, at 218 (citing Nicaragua, *supra* note 12).

156. Barkham, *supra* note 39, at 80. Attacks in which an enemy state's obvious objective is complete and utter network debilitation; launching an evident all-out war resulting in extensive destruction and significant loss of life; or a cyberattack that was a preliminary part of a kinetic attack would all likely be examples of armed attacks under Article 2(4) sufficient to trigger a right to self-defense under Article 51. *Id*. Note, however, that while these examples are obvious enough to satisfy attack-attribution, attacker-attribution remains unanswered.

157. *Id*. at 81.

158. *Id*. at 82. For example, states may attempt to justify the use of force on the grounds that cyberattacks by an enemy state are constantly looming. *Id*. This justification would seemingly allow for forceful self-defense at any time if the threat were always impending. This runs contrary to the U.N. Charter's express purpose of "maintain[ing] international peace and security." U.N. Charter.

159. Barkham, *supra* note 39, at 82.

160. *Id*.

161. Brenner, *Attribution and Response*, *supra* note 9, at 409. The widespread availability of computers and Internet access and the ability of cyberattackers to hide, disguise their online personas, and use "stepping stones" make this especially true. Villers, *supra* note 22, at 459–60.

upon it by a cyberattack, any response based on uncertain or incomplete information could result in disproportionate collateral damage or innocent civilian death.[162] In either case, retaliation based on imperfect information or without conclusive attribution will likely result in a violation of Article 51.

Attribution is not only necessary to prevent unlawful responses; it is necessary to ensure that some sort of response follows. Intermittent, small-scale cyberattacks could take advantage of the gap between Articles 2(4) and 51.[163] If cyberattacks are small enough, they might be considered a use of force but not an armed attack significant enough to

---

162. Barkham, *supra* note 39, at 82. This applies to both kinetic and electronic responses. *Id*. An example of this occurred in 1988, in which an Iranian Airbus was accidentally shot down because it was believed to be a military plane, resulting in 290 civilian deaths. *Id*. at 82–83; *see also* George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1179 (2000). Active defenses—electronic measures used to trace an attack back to its source and "disrupt it"—are commonly considered the most appropriate use of force against cyberattacks because they employ only necessary force and cause less disproportionate collateral damage. Sklerov, *supra* note 32, at 79–80. The problem with active defenses is that they are often engaged while a cyberattack is in progress. Barkham, *supra* note 39, at 82. A targeted state may have responded in self-defense without first determining the nature, scope, frequency, or effects of the attack. Thus, because the state did not determine attack-attribution, it does not know whether the initial cyberattack qualifies as an armed attack under Article 51. Furthermore, active defenses that shut down attacking computers could have unpredictable, cascading effects. *Id*. at 83. For example, if an active defense counterattacked an attacking system, it could penetrate an unmapped system. *Id*. Without mapping a system and knowing its contours, the operator might not be able to distinguish military targets from civilian targets. *Id*. Thus, without fully determining attack-attribution, the originally-targeted state could violate Article 51 and the principles of necessity and proportionality. *See* Ruth Wedgwood, *Proportionality, Cyberwar, and the Law of War*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 219, 227–30 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (arguing that it is more difficult to restrict the effects of active defenses than with kinetic weapons because connections from a target computer to the civilian infrastructure it controls are less evident; also arguing that there is insufficient time to map attacking systems when using active defenses, which could result in broad, unintended consequences). *But see* Michael Schmitt, *Wired Warfare: Computer Network Attack and the Jus in Bello*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 187, 204–05 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (arguing that active defenses merely shut down attacking computer systems for a brief time, rather than using kinetic weapons which cause widespread destruction to attain their objectives).

163. Barkham, *supra* note 39, at 83. In the previous section, there was discussion of local law enforcement responding to local cyberattacks which are ultimately part of a larger, coordinated attack. This is the other side of that coin—that is, uncoordinated cyberattacks insufficient in scope or character to qualify as an armed attack.

trigger the victim's right of self-defense under Article 51.[164] In contrast, a series of small-scale attacks might constitute an armed attack under Article 51, but local law enforcement might treat each attack as a separate incident rather than parts of a larger attack.[165] Although self-defense may be appropriate in the latter example, no response would ensue as no one would be aware of the larger attack.[166] Therefore, in the context of cyberattacks and cyberterrorism, attribution matters. Attributing the origin of a cyberattack and effects of an attack to a state are vital in complying with the requirements of self-defense under international law. The pervasiveness of nonstate actors on the Internet and their ability to disguise their tracks requires that the concept of attribution not only remain in place, but be reinforced. Thus, in order to prevent innocent deaths and collateral damage, "getting it right" is of extreme importance.

III. REINFORCEMENT OF ONLINE ATTRIBUTION

The main problems regarding online attribution are the lack of conclusive information and the need for absolute certainty. The anonymity of the Internet and the ability to disguise one's online persona create inherent difficulties in determining which state failed in its duty to prevent an attack from being launched within its borders.[167] Bifurcated response authority makes it difficult for military and civilian law enforcement to contemporaneously determine attack-attribution and coordinate a synchronized response.[168] However, online state attribution is of such importance that it must not be circumvented. Instead of getting rid of state attribution, measures should be taken to reinforce or ease the process of attributing a cyberattack to a state through increased cooperation and sharing of information, externally among states and internally among military and law enforcement personnel.[169]

---

164. *Id*. at 81. For example, if a series of small-scale incursions occur in another state's computer systems, causing few disruptions and minor damage, such incursions might not constitute an armed attack. *Id*. It may be likened to a state sending its troops across another state's border without causing any significant damage. *Id*.

165. Brenner, *Attribution and Response*, *supra* note 9, at 439.

166. *Id*.

167. Villers, *supra* note 22, at 459–60.

168. Brenner, *Attribution and Response*, *supra* note 9, at 441. Bifurcated response authority requires military personnel to respond to external threats, including acts of war, and law enforcement personnel to respond to internal threats, including crime and terrorism. *Id*. Further, civilians have no role in responding to crime or terrorism. *Id*. This response authority seems like a logical system probably because "it is all we know." *Id*.

169. While this Note proposes that states should be required to share information with other states and domestic law enforcement should share information with the military, Susan Brenner takes this concept one step further. *Id*. at 465–74. Professor Brenner pro-

While there is no silver bullet to solve the problems of online attribution, many different solutions have been proposed.[170] Requiring states to share information to conclusively determine attacker-attribution is consistent with the legal and practical limitations of state sovereignty, as the duty to cooperate can be found in several sources.[171] U.N. Member States are already under an obligation "[t]o achieve international co-operation in solving international problems . . . ."[172] Multilateral informal cooperation between states would not require any additional treaty processes and is crucial to the development of international cyberlaw.[173] Thus, states would not have any additional obligations placed on them; only reinforcement of an obligation that already exists.

A policy requiring internal state entities to cooperate and share information is consistent with legal and pragmatic constraints of the institutional separation of the military and law enforcement.[174] Specifically, law enforcement's contribution to the military would be providing informa-

---

poses integration of civilians, the military, and law enforcement personnel. *Id*. at 465. She suggests a voluntary organization to train and coordinate civilians in an attempt to support military and law enforcement efforts against cyberattacks. *Id*. at 469.

170. *Planning for the Future of Cyber Attack Attribution: Hearing Before the H. Comm. on Sci. & Tech.*, 111th Cong. (2010) (statement of Edward J. Giorgio, President, Ponte Technologies) [hereinafter *Planning for the Future*]; *see also* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSAT'L L. 57 (2010) (discussing giving every state universal jurisdiction to prosecute cyberterrorists as a means of deterrence); Jeffrey Hunker, *U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away*, 4 J. NAT'L SECURITY L. & POL'Y 197 (2010) (discussing improving the governance structure of the Internet, building norms for online behavior for states and individual users, and expanding multilateral cooperation against cybercrime).

171. Robert Uerpmann-Wittzack, *Principles of International Internet Law*, 11 GERMAN L.J. 1245, 1259–60 (2010) (discussing the existing "[p]rinciple of [i]nterstate [c]ooperation" in the context of internet law). For example, the duty of cooperation among states is found in the U.N. Charter, the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States, the Convention on the Rights of the Child, and the Convention on Cybercrime of 2001, to name a few. *Id*. at 1259.

172. U.N. Charter art. 1, para. 3.

173. Hunker, *supra* note 170, at 200; *see, e.g.*, Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, U.N. GAOR, 25th Sess. Supp. No. 28, U.N. Doc. A/8028 (Oct. 24, 1970) (U.N. General Assembly Resolution reinforcing the principles of cooperation among states for the furtherance of international peace and security).

174. Brenner, *Attribution and Response*, *supra* note 9, at 469.

tion about incidents that might constitute cyberwar, while the military would provide law enforcement about cybercrime and cyberterrorism.[175]

While states should be required to share information to assist one another in determining attacker- and attack-attribution, the rapidly evolving nature of technology may even render that obligation obsolete. The trend in technology is moving towards embedding identification and location tags deep into infrastructure, which will be difficult to circumvent.[176] Eventually, the infrastructure will provide authentication of the person at the other end of the signal rather than the person operating it.[177] However, until then, cyberattack attribution must remain in place.

CONCLUSION

This Note has explored the necessity of retaining the concept of attribution in the context of cyberattacks and cyberterrorism, even though some have called for its abolition.[178] The proliferation and abundance of computers and computer-related technologies has changed the safety and legal landscapes in unprecedented ways.[179] The widespread availability of computers and Internet access provides an unparalleled number of nonstate actors with the ability to launch cyberattacks on private, public, and military systems anywhere in the world.[180] International law, however, has evolved to hold states legally responsible for the acts of nonstate actors.[181] After the events of 9/11, international law grew to hold states indirectly responsible if they provide any support to persons involved in terrorist acts, including failure to prevent the launch of an attack.[182]

---

175. *Id*. The U.S. implemented the Homeland Security Act of 2002, which authorizes the Department of Homeland Security to share cyber security information with state and local governments, as well as private entities that maintain critical systems. Benjamin R. Davis, Comment, *Ending the Cyber Jihad: Combating Terrorist Exploitation on the Internet with the Rule of Law and Improved Tools for Cyber Governance*, 15 COMMLAW CONSPECTUS 119, 154 (2006).

176. *Planning for the Future*, *supra* note 170. New Internet protocols may also embed characteristics such as personal identity, hardware identity, location, and institutional affiliation. *Id*. A tag is a form of metadata, or a record of information, which captures the basic characteristics of data, resources, and the user. *Geospatial Metadata*, FED. GEOGRAPHIC DATA COMM., http://www.fgdc.gov/metadata (last visited Dec. 21, 2010).

177. *Planning for the Future*, *supra* note 170.

178. Proulx, *supra* note 9, at 643–53.

179. Brenner, *Attribution and Response*, *supra* note 9, at 474.

180. Villers, *supra* note 22, at 459–60.

181. Proulx, *supra* note 9, at 634–35.

182. Dantiki, *supra* note 83, at 655 (arguing that Resolution 1373 created a binding obligation on states to reform domestic law in order to more appropriately fight international terrorism).

Once an attack qualifies as an armed attack under Article 51 of the U.N. Charter, a victim-state is permitted to retaliate in self-defense, provided that the response conforms to the principles of necessity and proportionality.[183] Attribution in this context ensures that a victim-state responding in self-defense does not target innocent people or states and determines that the response is proportionate to the original attack.[184] The primary difficulty of attributing a cyberattack to a particular state is that the characteristics of an online attack do not hold the same significance as the characteristics of a kinetic attack.[185] In particular, places do not have any real value in online attacks because, although an attack may have been routed through a particular location, it does not mean the attack originated from that location.[186] Essentially anyone has the ability to launch an anonymous transnational cyberattack.[187] Determining the nature of an attack—and thus ensuring the response is proportional—is difficult because the indicators we rely on in real-world attacks—motive, location of attack, physical evidence—do not always exist in cyberattacks.[188] Bifurcated response authority and the ability of attackers to launch small-scale attacks, which may create communication and coordination problems among the military and law enforcement, further complicate the issue.[189]

The inherent difficulty in cyberattack attribution highlights why the concept of attribution is of extreme importance. The need for legal certainty requires that states attribute cyberattacks to the accurate state to prevent innocent deaths and unnecessary collateral damage. As such, the concept of online attribution should be reinforced through increased state collaboration and sharing of information. Such a requirement does not create any additional obligations on states. It is merely a reinforcement of an existing obligation of cooperation. Eventually, the technology will catch up with the law. Until then, the concept of cyberattack attribution must endure.

Levi Grosswald[*]

183. Jensen, *supra* note 25, at 218.
184. Brenner, *Attribution and Response*, *supra* note 9, at 405.
185. *Id*. at 409.
186. *Id*.
187. *Id*. at 412.
188. *Id*. at 435.
189. *Id*. at 438.

* B.S., University of Florida (2004); J.D., Brooklyn Law School (expected 2012). I am exceptionally grateful to my family and friends for their love, encouragement, and support. Special thanks to my parents, my brothers Seth and Matthew Grosswald, and Monica Lewis, who inspired me to keep writing when there was no end in sight. I would

also like to thank Hilary Dowling, without whom I still would not have a topic, and the staff and editors of the *Brooklyn Journal of International Law* for their dedication and hard work in helping me prepare this Note. All errors and omissions are my own.