Article

Attribution Issues in Cyberspace

Collin S. Allan*

Abstract

This article discusses one of the problems with the current condition of the international attribution regime. The rise of non-state actors in international and internal conflicts has created many problems for the international community. This is especially true in the case of cyber attacks. The tests for attributing the actions of a non-state actor to a state were devised before the age of the Internet and before cyber attacks accompanied armed attacks. The entities that conceived the attribution tests were unable to factor cyber attacks into their considerations because, in large part, the ability to conduct a cyber attack had yet to be developed. Cyber attacks can have a devastating impact on a state's economy and infrastructure. Because new technological developments allow non-state actors to launch cyber attacks, especially those implemented in conjunction with armed attacks, as was the case in Georgia in 2008, the international community should reassess where it stands on the issue of attribution.

This article uses the Georgia-Russia conflict as a window into the problems of attribution. It examines the attribution tests set forth in the International Court of Justice's Nicaragua decision, the International Criminal Tribunal for the Former Yugoslavia's Tadić decision, and Article 8 of the Draft Articles on Responsibility for Internationally Wrongful Acts. This article calls on the relevant parties to set a lower standard for attribution,

* Collin Allan recently graduated from BYU Law School. I wish to thank BYU Professor Eric Talbot Jensen for his guidance, experience, and support.

especially when a cyber attack occurs in conjunction with an armed attack.

Table of Contents

Attribution Issues in Cyberspace

Collin S. Allan

Introduction

The rise of non-state actors in international and internal conflicts has created many problems for the international community. This is especially true in the case of cyber attacks. Organized crime groups and individual civilians located in Russia provide examples of non-state actors that have played a major role in cyber attacks. While organized crime groups may traditionally be recognized for everything from human trafficking to grisly murders, one thing they are generally not known for is their participation in armed conflicts through cyber attacks aimed against the Russian government's enemies. The participation of individual civilians, sometimes referred to as hacktivists, in armed conflicts through cyber attacks is equally surprising. Specifically, Russian organized crime groups and individual civilians from Russia recently participated in the Georgia-Russia conflict. This participation has turned many people's attention to non-state actors' involvement in cyber warfare.

The background behind Russia's organized crime groups reveals the extent to which these groups have worked with the Russian government and raises legal questions of state attribution for actions taken by non-state actors. During Soviet times, organized crime initially made inroads shortly after the Communist revolution, peaking in the 1930s before diminishing due to infighting and state pressure.[1] Organized crime made a resurgence during Brezhnev's tenure, as different groups sought to increase ties with the government.[2] Under Gorbachev, the government began to implement decentralizing reforms, and organized crime groups "seized the opportunity to monopolize" industries abandoned by the government, "greatly expand[ing] their influence and financial base."[3]

With the collapse of the Soviet Union in the early 1990s, organized crime flourished in Russia, engaging in everything from human trafficking to violence to the drug trade.[4] During this time, organized crime groups expanded their influence into legitimate businesses as a cover for their

---

[1] Vsevolod Sokolov, *From Guns to Briefcases: The Evolution of Russian Organized Crime*, 21 WORLD POL'Y J. 68, 69 (2004).
[2] *Id.*
[3] *Id.* at 70.
[4] *Id.*

illegitimate activities.[5] Russian organized crime has largely left the realm of more base criminal pursuits, as crime bosses have transferred their financial holdings into more legitimate ventures.[6]

In his first term, Putin promised to crack down on organized crime.[7] Despite this promise, organized crime in Russia has maintained a transnational influence:[8] it has connections to organized crime in Western Europe, South America, and Asia.[9] Russian organized crime has taken advantage of "the opportunities for increased activity" due to globalization and the breaking down of boundaries between states due to advances in technology.[10] The truly frightening aspect of these developments, however, is organized crime's renewed influence.[11] In fact, it is such a problem that "[m]any within and outside of Russia see it as a national security issue for the Russian state."[12] With the evolution of Russia's organized crime and the spread of globalization, crime groups have diversified their activities and delved into cyber-crime.[13] One of their most influential forays took place during the Georgia-Russia conflict of 2008.

On the evening of August 7, 2008, the tension that had been building along the Russian-Georgian border for several months reached a head, resulting in an armed conflict between Russian and Georgian forces.[14] While people around the world watched clips of tanks and aircraft destroying buildings and wounding civilians, there was an aspect of the conflict that was not as readily apparent to the casual observer, newspaper-reader, or cable news-watcher: cyber attacks.

Cyber attackers within Russia launched the first of two phases of cyber attacks against Georgia on August 7, 2008, the same day that armed attacks began.[15] Cyber attackers, many of them civilians or hacktivists, targeted and shut down Georgian news and government websites, effectively cutting off Georgia from the rest of the world and the Georgian

---

[5] *Id.* at 70-71.
[6] *Id.*
[7] *Id.* at 71.
[8] Louise Shelley, *Contemporary Russian Organised Crime: Embedded in Russian Society, in* ORGANISED CRIME IN EUROPE: PATTERNS AND POLICIES IN THE EUROPEAN UNION AND BEYOND 563 (Cyrille Fijnaut & Letizia Paoli eds., Springer 2004).
[9] *Id.* at 563, 570, 576.
[10] Leslie Holmes, *Corruption and Organised Crime in Putin's Russia*, 60 EUROPE-ASIA STUDIES 1011, 1012 (2008).
[11] Shelley, *supra* note 8, at 571, 575-576, 579.
[12] *Id.*
[13] *Id.* at 577.
[14] C.J. Chivers, *In Georgia and Russia, A Perfect Brew for a Blowup*, N.Y. TIMES, Aug. 11, 2008, at A10, *available at* http://www.nytimes.com/2008/08/11/world/europe/11ticktock.html?_r=0.
[15] Paulo Shakarian, *The 2008 Russian Cyber Campaign Against Georgia*, 91 MILITARY REV. 63, 63 (2011).

people from any crucial information they may have obtained from their government.[16] The botnets used to carry out the distributed denial of service ("DDoS") attacks were affiliated with Russian organized crime groups, including the Russian Business Network ("RBN"), a criminal organization known to use and lease botnets for criminal purposes.[17] This conflict marked the first time that a large-scale cyber attack was "conducted in tandem with major ground combat operations."[18]

With the rise and increasing participation of non-state actors in attacks throughout the world against states, many wonder how the Law of Armed Conflict ("LOAC") can or should apply to non-state actors.[19] This question is especially relevant when attacks occur in cyberspace because of the difficulty in determining the concrete identity of cyber attackers or the origins of the attack.[20] For example, in 2007, Estonia was the victim of crippling cyber attacks.[21] A search for the origin of the attacks led experts not only to Russia and several Russian government institutions, but also to 177 other countries.[22] While the 2008 cyber attacks in Georgia were not the first cyber attacks against another state, they marked the first time such an attack occurred in concert with an armed attack against another state.[23] Furthermore, they marked the first time that a state either coincidentally or intentionally employed non-state actors to conduct a cyber attack in tandem with its armed attack.

The combined nature of cyber and armed attacks raises many legal questions. This article focuses on the question of state responsibility and explores how much control a state must exert over non-state actors before the actions of those non-state actors becomes imputable to the state, using

---

[16] *Id.*
[17] *Id.* at 64.
[18] *Id.* at 63; John Markoff, *Before the Gunfire, Cyber Attacks*, N.Y. TIMES, Aug. 13, 2008, at A1, *available at* http:// www.nytimes.com/2008/08/13/technology/13cyber.html.
[19] *See* Carina Bergal, *The Mexican Drug War: The Case for a Non-International Armed Conflict Classification*, 34 FORDHAM INT'L L.J. 1042 (2011); Norman G. Printer, Jr., *The Use of Force Against Non-state Actors Under International Law: An Analysis of the U.S. Predator Strike in Yemen*, 8 UCLA J. INT'L L. & FOREIGN AFF. 331 (2003); William Schabas, *Punishment of Non-State Actors in Non-International Armed Conflict*, 26 FORDHAM INT'L L.J. 907 (2003).
[20] *See* Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 570, 594-595 (2011).
[21] *Id.* at 569.
[22] *Id.* at 570.
[23] Shakarian, *supra* note 15, at 63; Markoff, *supra* at note 18, at A1. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009). Not only have Estonia and Georgia been the victims of cyber attacks within the past eight years, but Lithuania and Kazakhstan have also been victims of cyber attacks. U.S. Cyber Consequences Unit Special Report, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, 1 (Aug. 2009), http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

the Georgia-Russia conflict as an example. The main goal of this article is not to assign blame in the Georgia-Russia conflict, but rather to explore the current condition of attribution and its application to cyber warfare, especially when cyber attacks are conducted in concert with a kinetic attack.

The International Law Commission's ("ILC") Draft Articles on the Responsibility of States for Internationally Wrongful Acts ("Draft Articles on State Responsibility") summarize the current tests for state responsibility. These tests are articulated in the International Court of Justice's ("ICJ") *Military and Paramilitary Activities In and Against Nicaragua* case ("*Nicaragua"*), and the International Criminal Tribunal for the Former Yugoslavia's ("ICTY") *Prosecutor v. Tadić* case ("*Tadić"*). The ILC's Draft Articles on State Responsibility deal with the principal of control in general, and, in the Articles' commentary, the ILC looks to both *Nicaragua* and *Tadić* for articulations of control tests. *Nicaragua* and *Tadić* examine control as it deals with a state's control over armed groups.

Because the proliferation of cyber attacks are post-*Nicaragua* and *Tadić* developments, the courts deciding those cases did not include cyber attacks in their determinations. The Georgia-Russia conflict exemplifies the difficulty in applying the control tests to a conflict that includes cyber attacks. The differences in the way that kinetic attacks are carried out, as opposed to the way cyber attacks are conducted, make it difficult for tests designed to apply to armed groups and civilians carrying out physical acts through kinetic warfare to apply to attacks that take place in cyberspace. Because of these differences and the attendant issues that arise in a cyberspace attack, the international community should consider a new test for addressing the issue of attribution when cyber attacks occur in tandem with an armed attack. Currently, the tests set an unworkably high bar in determining when a state may be responsible for the actions of a non-state actor, given the context of cyber attacks. This test must lower the required degree of connection between a state and a non-state cyber attacker before a state may be responsible for the non-state cyber attacker's actions.

Section I of this article begins to discuss the need for a new test to measure state responsibility by examining the factual framework of the 2008 Georgia-Russia conflict. Section II discusses the current attribution regime as developed in *Nicaragua*, *Tadić*, and Article 8 of the Draft Articles on State Responsibility. Section III explores the application of the current attribution regime and other relevant international law to 2008 Georgia-Russia, highlighting the problems of the existing legal regime. Finally, Section IV continues to discuss problems with the current

attribution regime and asserts possible solutions, or at least potential positive changes.

I. The Georgia-Russia Cyber Conflict: A Two-Pronged Attack

The details surrounding the kinetic and cyber conflicts between Russia and Georgia are unclear at best. There is still speculation as to which party initiated the cyber attacks against Georgia and no hard evidence as to the Russian government's level of involvement. The exact identity of who orchestrated the cyber attacks is unknown. Georgia blames Russian government for the attacks, but the Russian government denies all accusations.[24] While it is not clear who was behind the cyber attack, American computer security researchers "saw clear evidence of a shadowy St. Petersburg-based criminal gang known as the . . . RBN."[25] The following are the facts as experts have discussed and written them.

From the beginning of the conflict, Georgia faced a two-pronged attack.[26] The first prong employed conventional means: tanks, aircraft, missiles, and bullets. The second prong was an unprecedented cyber attack that coincided with the conventional attack, targeting the Georgian government and business websites.[27] Attacks on businesses and financial institutions caused international financial institutions to cut off operations with Georgian banks.[28] One purpose for the attacks may have been to cause economic damage.[29] Additionally, the attacks had "a significant informational and psychological impact on Georgia."[30] The attacks disabled cellphone services throughout the country and "effectively isolated [Georgia] from the outside world."[31] The Russian armed forces benefited from the cyber attacks. For example, Russian armed forces did not attack Georgian "media and communication facilities," which may have been due to the success of the cyber attacks.[32]

The first phase of the cyber attack consisted of Russian cyber attackers launching DDoS attacks.[33] The purpose of a DDoS is "to prevent

---

[24] Markoff, *supra* note 18.
[25] *Id.*
[26] Chivers, *supra* note 14; Markoff, *supra* note 18.
[27] Markoff, *supra* note 18.
[28] Shakarian, *supra* note 15, at 65-66.
[29] *Id.*
[30] *Id.* at 63.
[31] *Id.*
[32] *Id.* at 65.
[33] Shakarian, *supra* note 15, at 63.

the legitimate use of a computing source."[34] During this initial phase, the DDoS attacks were primarily carried out by botnets, "a group of computers on the Internet . . . that have been infected with a piece of software known as malware."[35] Criminal organizations, including the RBN, are known to "use and lease botnets for various purposes."[36] The botnets used in the attack against Georgia were "affiliated with Russian criminal organizations, including the RBN."[37] Cyber security experts stated that in some cases, the attacks originated from computers known to be controlled by the RBN.[38] During the second phase of the attack, the cyber campaign expanded from government targets to include "financial institutions, businesses, educational institutions, Western media . . . and a Georgian hacker website."[39]

Questions regarding whether the RBN coordinated with or were under the control of the Russian government remain unsettled.[40] However, experts believe the fact that the attacks occurred only "one day prior to the ground campaign" indicates "that the hackers knew about the date of the invasion beforehand."[41] There is little hard evidence of coordination beyond the close timing of both the conventional attack and the cyber attack.[42] The Russian government has not accepted responsibility for the attacks, nor has it formally approved of them. Colonel Anatoly Tsyganok, the head of the Russian Military Forecasting Center, in discussing this conflict, was careful not to attribute the cyber attacks to the Russian government.[43] Nonetheless, he described the cyber campaign "as part of a larger information battle with Georgian and Western media."[44]

While Russian organized crime groups provided the means for the attacks, including the malware and advice on how to carry out the attacks, and conducted many of the attacks themselves, they made up only one group of those involved in the cyber attacks against Georgia.[45] "Patriotic" Russian civilians, likely using personal computers, also comprised a large

---

[34] *Id.*
[35] *Id.*
[36] *Id.* at 64.
[37] *Id.*
[38] Markoff, *supra* note 18.
[39] Shakarian, *supra* note 15, at 64.
[40] Markoff, *supra* note 18.
[41] Shakarian, *supra* note 15, at 64.
[42] *Id.* at 66.
[43] *Id.* at 65.
[44] *Id.*
[45] Shakarian, *supra* note 15, at 63-64.

number of cyber attack participants.[46] Therefore, while the organized crime groups in large part provided the means for the attacks, these civilian Russian sympathizers, termed "hacktivists,"[47] actually carried out the attacks.[48] The civilians were able to carry out the attacks by visiting various websites, which contained "user-friendly button[s]" and provided instructions that "were very accessible, even for a novice user."[49] One cite had a button labeled "'FLOOD' which, when clicked, deployed multiple DDoS attacks on Georgia."[50]

II. The Law Governing Attribution

Any connection between the organized crime groups and Russia that would establish Russian responsibility for the cyber attacks must derive from international law. The ILC's Draft Articles on State Responsibility summarize this law. The *Nicaragua* and *Tadić* cases articulate the tests used to determine what level of control is necessary before a state becomes responsible for the actions of non-state actors. Article 8 of the Draft Articles on State Responsibility discusses the principle of imputing a non-state actor's actions to the state.[51] The commentary to this article expounds on the text. In *Nicaragua*, the ICJ discussed how much and what kind of control a state needs to exert over a non-state actor in order for the non-state actor's actions to be attributed to the state.[52] Additionally, the ICJ formulated the "effective control test" in *Nicaragua*.[53] The ICTY discussed the same principle in *Tadić*.[54] However, the ICTY rejected the ICJ's effective control test and concluded that the lower standard of overall control was sufficient to attribute a non-state actor's actions to the state.[55]

---

[46] U.S. Cyber Consequences Unit Special Report, *supra* note 23, at 2-3; Noah Shachtman, *Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It*, WIRED NEWS (Mar. 11, 2009), http://www.wired.com/dangerroom/2009/03/georgia-blames/; Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. Rev. 43, 64 (2009).
[47] Shakarian, *supra* note 15, at 64.
[48] U.S. Cyber Consequences Unit Special Report, *supra* note 23, at 3.
[49] Shakarian, *supra* note 15, at 64.
[50] *Id.*
[51] Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, art. 8, U.N. Doc. A/56/10 (Nov. 2001).
[52] Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), 1986 I.C.J. 14 (June 27).
[53] *Id.* ¶ 115.
[54] Prosecutor v. Tadić, Case No. IT-94-1-A (Int'l Crim. Trib. for the Former Yugoslavia Jul. 15, 1999).
[55] While the ICJ's advisory opinion on the construction of the wall in Palestinian territory by Israel arguably addressed effective control, its decision does not fall within the purview of this article. The

A. Article 8 of the Draft Articles on State Responsibility

Article 8 of the ILC's Draft Articles on State Responsibility states that the "conduct of a person or group of persons shall be considered an act of a State under international law" in two situations: when a person or people are acting "on the instructions of" that state, or when a person or people are acting under "the direction or control of" the state.[56] The purpose of Article 8 is to single out states that employ private individuals to carry out activities that would be inappropriate for the states or their officials to engage in.[57] Therefore, a state cannot avoid responsibility by having a private individual or group of private individuals do the state's "dirty work." The commentary on the draft articles explores the legal underpinnings of the article and, in large part, turns to both *Nicaragua* and *Tadić* for guidance.

The commentary for Article 8 begins by stating that the general rule in international law is that a state will not be responsible for the actions of private persons or private entities.[58] It goes on to say, however, that the existence of a "specific factual relationship" between the state and a person or group of people may create a circumstance where the actions of those non-state actors are attributed to the state.[59] The commentary analyzes the two situations when these circumstances may arise.[60]

First, when a person or group of people acts on the instructions of a state, it is accepted that the state has authorized those actions.[61] When a state has authorized conduct, international jurisprudence often attributes

---

ICJ determined that Israel was not seeking to attribute the terrorist attacks to a state, but rather, Israel stated that the attacks arose from within this territory, constituting a threat to Israel's security. Because Israel was not attempting to attribute the attacks to a state, this case does not fall within the context of this article (*see* Legal Consequences of Construction of Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, 138-140 (July 9)). Furthermore, because the attacks in Israel were arising within territory that Israel claimed to control and not from outside if this territory, a factual distinction arises between that case and the Georgia-Russia conflict.

[56] Int'l Law Comm'n, *supra* note 49. Articles 4 and 5 also address state responsibility. Article 4 addresses responsibility for the actions of a state's organs. Article 5 addresses non-state actors that are empowered by the state to "exercise elements of the governmental authority." However, because the facts seem fairly clear that the cyber attacks were perpetrated by groups that were neither government organs nor empowered to exercise elements of government authority, these articles will not be considered in detail in this article. Rather, it seems to be clear that organized crime groups and civilians carried out the acts.

[57] Tadić, *supra* at 54, ¶ 117.

[58] Int'l Law Comm'n, *supra* note 51, art.8, cmt. 1.

[59] *Id.*

[60] *Id.*

[61] *Id.*

that conduct to the state, even if the people involved are private individuals and even if their conduct does not involve "'governmental activity'" per se.[62] The rational is that when a person or group of people has a state's authorization to do something, they become a de facto organ of that state.[63] Most often, this will occur when a state or one of its organs recruits private groups to perform activities or missions outside its borders.[64]

In the second situation, it is more difficult to attribute conduct to a state when the actions were carried out "'under the direction or control' of a State."[65] If an individual or group of people act "under the direction or control of a State," that conduct will be attributed to the state.[66] However, conduct "will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation."[67] If the conduct was only incidental or peripheral to the operation, then this principle does not extend to that conduct.[68] The commentary, unfortunately, does not discuss the difference between integral involvement and mere incidental or peripheral involvement. However, it does briefly discuss the *Nicaragua* and *Tadić* cases, as they constitute Article 8's legal origin.

B. Nicaragua and The Effective Control Test

In *Nicaragua*, the ICJ established the effective control test as a means to determine whether the actions of a non-state actor can be attributed to a state based on the level of control that state exercises over the non-state actor.[69] The ICJ looked at the United States' involvement in the conflict between the *contras* and the Sandinistas during the 1980s to determine whether the U.S.' actions reached a sufficient level of control over the *contras* to attribute the *contras*' actions to the U.S.[70]

The ICJ wrestled with the degree of control the United States needed to exert over the *contras* before responsibility for the *contras*' actions could be attributed to the United States.[71] Nicaragua attempted to

---

[62] *Id.* cmt. 2.
[63] Tadić, *supra* note 54, ¶ 104.
[64] Int'l Law Comm'n, *supra* note 51, art. 2.
[65] *Id.* cmt. 3.
[66] *Id.* cmt. 1.
[67] *Id.*
[68] *Id.*
[69] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ ¶ 109, 115 (June 27).
[70] *See id.*
[71] *Id.* ¶ 113.

attribute the *contras*' actions to the United States in order to show that the United States had violated an obligation of international law "not to kill, wound or kidnap citizens of Nicaragua."[72] Nicaragua claimed the United States government "devised the strategy and directed the tactics of the *contra* force, and provided direct combat support for its military operations."[73] Nicaragua relied on the correlation between the timing of repeated receipt of new funds from the United States and a subsequent offensive by the *contras,*[74] the supply of aircraft, intelligence assistance, and tactical directions provided by United States personnel.[75] The United States admitted the "nature, volume, and frequency" of its financial support.[76]

The ICJ stated that "in light of the evidence and material available to it, [it was] not satisfied that *all* the operations launched by the *contra* force, at *every* stage of the conflict, reflected strategy and tactics *wholly* devised by the United States."[77] In its opinion, the ICJ did not downplay the U.S.' support and openly admitted that a number of operations were "decided and planned . . . at least in close collaboration" with U.S. advisors.[78] The ICJ also determined that although the United States did not create the *contra* force, it "largely financed, trained, equipped, armed and organized" at least one of the *contra* groups.[79]

Despite this, it *again* held that not "*all contra* operations reflected strategy and tactics *wholly* devised by the United States."[80] Furthermore, the ICJ also determined that the United States did not give "direct and critical combat support."[81] The ICJ interpreted "direct and critical combat support" to mean that the support provided by the United States "was tantamount to direct intervention by the United States combat forces."[82]

In determining that the *contras* actions could not be attributed to the U.S., the ICJ reasoned in the following manner:

> The Court has to determine . . . whether or not the relationship of the *contras* to the United States

[72] *Id.*
[73] *Id.* ¶ 102.
[74] *Id.* ¶ 103.
[75] *Id.* ¶ 104.
[76] *Id.* ¶ 107.
[77] *Id.* ¶ 106 (emphasis added).
[78] *Id.*
[79] *Id.* ¶ 108.
[80] *Id.* (emphasis added).
[81] *Id.*
[82] *Id.*

> Government was so much one of *dependence* on the one side and *control* on the other that it would be right to *equate* the *contras*, for legal purposes, with an organ of the United States Government, or as acting on behalf of that Government.[83] . . . . [D]espite the heavy subsidies and other support provided to them [the *contras*] by the United States, there is no clear evidence of the United States having actually exercised such a degree of control in all fields as to justify treating the *contras* as acting on its behalf.[84]
>
> . . . .
>
> All forms of United States participation mentioned above, and even the general control by the respondent State over a force with a high degree of dependency on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State.[85]

In *Nicaragua*, the ICJ established a high standard for imputing responsibility of a non-state actor's actions to a state: the effective control test. The effective control test requires a state to essentially be in total control of the non-state actors, and the state must specifically direct or enforce violations of international law. The ICJ's use of the terms "wholly devised" when referring to strategy and tactics, "all" when referring to the operations launched by the *contras,* and "every" when referring to the stages of the conflict shows that the ICJ's effective control test requires near total control of the non-state actor throughout the entire conflict and execution of operations.[86] Subsequent decisions by international tribunals, most notably the ICTY in *Tadić*, and scholarly articles[87] have cast doubt on the efficacy of the effective control test.

C. Tadić and The Overall Control Test

Tadić was decided in 1999, more than ten years after the

---

[83] *Id.* ¶ 109.
[84] *Id.* ¶ 109 (emphasis added).
[85] *Id.* ¶ 115.
[86] *Id.* ¶ 106.
[87] *See* Antonio Cassese, *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 EUR. J. INT'L L. 649, 653-55 (2007).

Nicaragua case.[88] However, the issues of how and when to hold a state accountable for the actions of non-state actors returned in *Tadić*.[89] The ICTY developed the overall control test and lowered the level of necessary control from that required by *Nicaragua*.[90] *Tadić* distinguished between two types of non-state actors and the level of control needed for each: (1) actors organized into a military structure; and (2) actors not organized into a military structure.[91] The ICTY determined that the necessary level of control is higher for the second group than for the first.[92]

The ICTY first examined militarily structured groups in its discussion of the soundness of *Nicaragua*'s effective control test. The ICTY described these groups as "organised and hierarchically structured."[93] These groups tend to have "a chain of command and a set of rules as well as the outward symbols of authority."[94] It determined that the effective control test, as established by the ICJ, was not an appropriate test in determining whether a state could be held responsible for the actions of militarily structured groups supported and assisted by the state because the effective control test was "at variance" with logic, judicial practice, and state practice.[95] Instead, the ICTY proposed the overall control test for individuals organized as a militarily structured group.[96]

The ICTY turned to other international tribunals to show widespread reliance on a less stringent test than the effective control test propounded in *Nicaragua*.[97] In its discussion of a Mexico-United States General Claims Commission case, the ICTY noted that "the Commission did not enquire as to whether or not specific instructions had been issued concerning" the internationally unlawful act committed by a member of the Mexican irregular army.[98] In that case, the Commission held Mexico responsible for the actions of the non-state actor.[99] This was one example that demonstrated that other international tribunals had established a lower standard than that required by the effective control test.

The ICTY next turned to an Iran-United States Claims Tribunal

---

[88] Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment, ¶ 120 (Int'l Crim. Trib. for the Former Yugoslavia Jul. 15, 1999).
[89] *Id.* ¶ 98.
[90] *Id.* ¶¶ 116-120.
[91] *Id.* ¶ 120.
[92] *Id.* ¶ 137.
[93] *Id.* ¶ 120.
[94] *Id.*
[95] *Id.* ¶¶ 116, 124.
[96] *Id.* ¶ 131.
[97] *Id.* ¶ ¶ 125-30.
[98] *Id.* ¶ 125.
[99] United States v. Mexico, Reports of International Arbitral Awards, vol. IV, pp. 266- 267.

case that discussed a military group who enforced the law, forced Americans to leave their homes, detained those Americans in a hotel, and searched them at an airport.[100] The ICTY concluded the non-state actors were "performing *de facto* official functions,"[101] that is, functions that are generally solely within the purview of state authority. The ICTY emphasized that the state was held responsible for the actions of this group absent "specific instructions" from the state.[102] Despite the lack of instructions from the state, the ICTY noted that the tribunal concluded that when a military group acts as though it were a de facto state organ, the state will be responsible for the actions of that group.[103] Both of these examples show that courts have not necessarily focused on whether specific instructions were issued regarding the internationally unlawful acts. Rather, the second court looked at whether a non-state actor was performing state functions and how the state responded.

In the end, the ICTY determined that to impute the acts of a militarily organized group to a state, it "must be proved that the State wields overall control over the group."[104] A state does this, according to the ICTY, "by equipping and financing the group" and "by coordinating or helping in the general planning of its military activity."[105] It is not, however, necessary for the state to issue "instructions for the commission of specific acts contrary to international law."[106]

The location of unlawful acts and the location of the state also mattered to the ICTY; it stated that if the unlawful acts are committed in the territory of a state other than the controlling state, then "more extensive and compelling evidence" is needed to show the state "is genuinely in control . . . not merely by financing and equipping them, but also by generally directing or helping plan their actions."[107] However, if the conflict is between two adjacent states and the controlling state is attempting to expand its territory "through the armed forces which it controls, it may be easier to establish the threshold."[108]

After discussing groups organized in a military structure, the ICTY turned to groups not organized by military structures.[109] As the ICTY did

---

[100] Tadić, *supra* note 54, ¶ 126.
[101] *Id.* ¶ 127.
[102] *Id.*
[103] *Id.* ¶ 126.
[104] *Id.* ¶ 131.
[105] *Id.*
[106] *Id.*
[107] *Id.* ¶ 138.
[108] *Id.* ¶ 140.
[109] *Id.* ¶ 132.

with militarily organized groups, it discussed the deliberations of other international tribunals that investigated the same issues as those at hand in *Tadić*.[110] In the *United States Diplomatic and Consular Staff in Tehran* case decided by the ICJ, the ICTY argued that the ICJ correctly determined that the Iranian students who had taken members of an embassy staff hostage "had not initially acted on behalf of Iran" because the "Iranian authorities had not specifically instructed them to perform those acts."[111] However, after "Iranian authorities formally approved and endorsed the occupation of the Embassy," the students became "*de facto* agents of the Iranian State and their acts became internationally attributable to that State."[112]

In discussing the issue of control, as analyzed by the ICJ in the *Nicaragua* case, the ICTY stated that "it was deemed necessary by the Court that these persons not only be paid by United States organs but also act 'on the instructions' of those organs (in addition to their being supervised and receiving logistical support from them)."[113] The ICTY determined that a higher level of control was necessary for non-militarily structured groups than for militarily organized groups.[114] For individuals or groups of individuals not organized into military groups, the ICTY suggested a higher standard: "[C]ourts have not considered an overall or general level of control to be sufficient [with regard to non-militarily organized groups], but have instead insisted upon specific instructions or directives aimed at the commission of specific acts, or have required public approval of those acts following their commission."[115]

In sum, the ICTY determined that the "extent of requisite State control varies" depending on the circumstances."[116] To determine whether an individual or group that is not militarily organized "has acted as a *de facto* State organ when performing a specific act, it is necessary to ascertain whether specific instructions concerning the commission of that particular act had been issued by that State to the individual or group in question."[117] Furthermore, sufficient control may also be established if, after the unlawful act has been perpetrated, the state "publicly endorse[s] or approve[s]" the actions taken.[118]

---

[110] *Id.* ¶ ¶ 33-35.
[111] *Id.* ¶ 133.
[112] *Id.*
[113] *Id.* ¶ 134.
[114] *Id.* ¶ 137.
[115] *Id.* ¶ 132.
[116] *Id.* ¶ 137.
[117] *Id.*
[118] *Id.*

For militarily structured groups, the overall control test is a lower standard than the effective control test. A state must not only finance and equip such military group, but also help or coordinate in the general planning of the non-state actor's military activities.[119] Specific instructions regarding the execution of internationally unlawful actions are not necessary.[120] This is a lower standard than the effective control test that required the strategy and tactics to be wholly devised by the controlling state.[121] The effective control test also required the controlling state's whole involvement in the development of military tactics and strategy at every stage of the conflict.[122] The overall control test only requires involvement in general planning.[123]

III. Analysis of Attribution in the Georgia-Russia Cyber Conflict

This section first discusses whether a breach of international law occurred in the Georgia-Russia situation. This is a threshold question that needs to be addressed before the control test analysis, as a discussion of state responsibility is irrelevant without a non-state actor's violation of international law. This section then applies the tests to the available facts of the Georgia-Russia situation.[124]

A. Was There a Breach of International Law?

Whether there was a breach of international law by a non-state actor is the threshold question for both the effective control and overall

---

[119] *Id.* ¶ 131.
[120] *Id.* ¶¶ 127, 131.
[121] Nicaragua, *supra* note 69, ¶ 106.
[122] *Id.*
[123] Tadic, *supra* note 88, ¶ 131.
[124] There are myriad related legal topics that deserve to be addressed when discussing the participation of non-state actors in an armed conflict, especially when that participation takes the form of a cyber attack. For example, the status of non-state participants in an armed conflict is an issue that demands further exploration. For the purposes of this article, however, the Russian organized crime groups and hacktivists, similar to the armed groups in *Tadić*, will not be considered "part of [the] armed forces" of a party to the conflict. (Tadić, *supra* note 88, ¶ 92.) Neither do they belong to a party to the conflict and satisfy the other four requirements provided for in the Third Geneva Convention of 1949 Article 4a(2): "(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; [and] (d) that of conducting their operations in accordance with the laws and customs of war." (Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949 ("Geneva Convention III" or "Third Geneva Convention"). Many legal questions arise from this, including: how do cyber troops wear uniforms or carry their arms openly? How can international law apply if, in most cases, it does not even apply to cyber conflict?) However, the topic of the non-state participants' status in this conflict, and other tangential topics, are beyond the scope of this article.

control tests. Without a breach of international law there is no reason to consider whether a state is responsible for the actions of a non-state actor. Because this article focuses on the actions of non-state actors, it is unnecessary to discuss whether the Russian troops' presence in Georgia breached international law.

With regard to the UN Charter, one scholar aptly noted that "cyber-warfare will challenge and test the Charter's bounds."[125] While there has not been a concrete determination as to how, or even if, a cyber attack breaches international law, the Russian hackers' actions are most likely to qualify as a breach of international law if their actions constituted a use of force, as described by the UN Charter, against Georgia.[126] Some scholars argue that a concrete interpretation of Article 2(4) of the UN Charter should be applied to cyber attacks, while others contend that specific treaties on cyber attacks would prove more useful.[127] One scholar has suggested that a more precise definition of the term "cyber attack" would solve many problems in this area.[128]

The writings of international scholars have created a spectrum of unlawfulness on which different cyber attacks can fall depending on their intensity.[129] On one end of the spectrum, there is the general prohibition of intervention as discussed in the 1981 UN General Assembly Declaration of Non-intervention.[130] The idea of non-intervention states that because states are sovereign, each state has the authority and is solely responsible for actions that take place within the boundaries of that state, and other states should not interfere or intervene in domestic issues.[131] In this case, non-intervention assumes that states are competent to deal with the cyber issues that arise within their borders. On the other end of the spectrum, a cyber attack has been defined as a use of force under the UN Charter only if the effects of the attack are similar to those that result from kinetic warfare.[132] From one point of view, to qualify as armed attacks, the "cyber operations must be severe enough . . . to result in damage to or destruction of property or injury to or death of individuals."[133] Economic coercion and political

---

[125] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 431 (2011).
[126] U.N. Charter art. 2, ¶ 4.
[127] Waxman, *supra* note 125, at 431.
[128] *See* Graham Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 87 (2009).
[129] *See* Marco Roscini, *World Wide Warfare - Jus ad bellum and the Use of Cyber Force*, MAX PLANCK UNYB 14, 103 (2010); Schmitt, *supra* at note 20, at 573.
[130] Roscini, *supra* at note 128, at 103.
[131] *Id.*
[132] *See* Schmitt, *supra* note 20, at 573; *see also* Roscini, *supra* note 129, at 103-109.
[133] Schmitt, *supra* note 20, at 602.

coercion are insufficient.[134] But, a cyber attack that has similar non-kinetic consequences to a kinetic attack may be sufficient.[135] For example, if a country's "Stock Exchange or other financial institutions were to be bombed and the markets disrupted as a consequence," this would qualify as a use of armed force.[136] In this example, the "economic consequences or the action would by far outweigh the physical damage to the buildings."[137] For some scholars, a cyber attack that achieved the same results would likely be considered a use of force if it, indeed, achieved results similar to those caused by dropping a bomb on the stock exchange.[138]

In Georgia, the cyber attacks fall onto different areas along the unlawfulness spectrum, depending on the perspective one takes. The cyber attacks from Russia against Georgia targeted government websites, business and financial institutions, educational institutions, and media outlets. The attacks isolated the country from the rest of the world and Georgian citizens from their government. The indirect effect of the attacks aided the Russian military in accomplishing its mission to protect Russian interests in South Ossetia and Abkhazia. The cyber attacks disrupted Georgian communications and generally caused confusion among the Georgian government and civilians in a way that allowed the Russian military to more effectively operate. The cyber attacks also disrupted Georgian markets by effectively shutting down Georgia's financial system when the cyber attacks caused outside banks to refuse to operate within the country. For these reasons, this article assumes Russia's cyber attacks against Georgia met the bar for use of force and breached international law.

B. Applying the Tests for State Responsibility

1. Russian Responsibility Under Article 8

Article 8, the effective control test, and the overall control test set a high bar for attributing responsibility of the internationally wrongful acts committed by a non-state actor to a state. The difficulty in reaching that bar is exacerbated when the misdeeds of the non-state actor are committed in cyberspace and not through kinetic means. Because of the relatively recent emergence of cyber attacks on the international stage, the ILC, ICJ, and ICTY have yet to consider cyber warfare in their control and

[134] Roscini, *supra* note 129, at 105.
[135] *Id.* at 108.
[136] *Id.* at 107-08.
[137] *Id.* at 108.
[138] *Id.* at 108.

responsibility determinations. The current attribution regime proves unworkable and a new attribution regime should be developed for cyber attacks.

Under Article 8, a state is responsible for the actions of a non-state actor when the non-state actor is acting "on the instructions of, or under the direction or control of, that state in carrying out the conduct."[139] The "acting on the instructions" element of Article 8 requires non-state actors to act on instructions received from the state to impute responsibility to the state.[140] With regard to the Georgia-Russia conflict, many experts believe that the time nexus between the conventional attack and the cyber attacks demonstrated that the cyber attackers, at the very least, knew an attack was going to be launched.[141] However, mere knowledge of an attack does not constitute "acting on instructions" from the state pursuant to Article 8.[142] Had the Russian government instructed the groups to conduct the cyber attacks or officially sanctioned them after the fact, it would have been tantamount to authorizing the attacks.[143] Concurrence in time between conventional and cyber attacks alone is not enough to establish specific factual relationship required by Article 8.[144] Without more knowledge of what actually took place between the Russian government and the cyber attackers it is extremely difficult to say that the Russian government authorized the attacks.

2. Russian Responsibility Under the Effective Control Test

The ICJ's effective control test requires that a state "actually exercise such a degree of control in *all* fields as to justify treating" the non-state actor "as acting on its behalf."[145] The court required the state to wholly devise the non-state actor's strategy and tactics; financing and equipping non-state actors is insufficient to establish state responsibility.[146] The ICJ also required the state to exert near total control over the non-state actors in conducting operations.[147] Direct and critical combat support from the state to the non-state actor is essential in meeting the effective control

---

[139] Int'l Law Comm'n, *supra* note 51.
[140] Int'l Law Comm'n, *supra* note 51, art.8, cmt. 1.
[141] U.S. Cyber Consequences Unit Special Report, *supra* note 23, at 3.
[142] Int'l Law Comm'n, *supra* note 51, art.8, cmt. 1,2,7.
[143] *Id.* art. 8, cmt. 1-7.
[144] *Id.* art. 8, cmt. 7.
[145] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 109 (June 27).
[146] *Id.* ¶ 106.
[147] *Id.* ¶ 109.

test.[148]

As applied to the Georgia-Russia conflict, the effective control test would not result in Russian responsibility for the cyber attackers' activities due to difficulty in establishing a connection between the state and the non-state actors.[149] In fact, no communication between the Russian government and the organized crime groups has been discovered.[150] If the Russian government is indeed behind the cyber attacks, the lack of hard evidence allowed them to circumvent Article 8's undergirding policies by successfully supporting non-state actors' cyber attacks against Georgia during an armed conflict.

Additionally, in the Georgia-Russia conflict, the few facts available tend to show that the Russian government did not exercise effective control over either group conducting the cyber attacks. The means of the attacks - the botnets and sites made available to hacktivists - were provided by the organized crime groups, not the state.[151] Furthermore, by all accounts, the Russian government did not provide direct and critical combat support to the cyber attackers.[152] If anything, the cyber attackers provided direct combat support to the Russian troops by disabling the Georgian government's ability to communicate with its citizens. For example, "media and communication facilities were not attacked by kinetic means," possibly because the cyber attackers had already carried out attacks against them and disabled them.[153] Due to the apparent lack of near total control exerted by the Russian government over the organized crime groups, the effective control test would not hold Russia accountable for the cyber attackers' activities.

3. Russian Responsibility Under the Overall Control Test

When applying the overall control test, it is first necessary to determine whether the cyber attackers fit within the definition of a militarily structured group.[154] If the cyber attackers can be defined as a militarily structured group, the overall control test of *Tadić* would apply. Under *Tadić*, Russian organized crimes groups would have to demonstrate

---

[148] *Id.* ¶ 108.
[149] Shakarian, *supra* note 15, at 66.
[150] *Id.*
[151] *Id.* at 63-64.
[152] *Id.* at 63-64, 66.
[153] *Id.* at 66.
[154] Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment, ¶ 120 (Int'l Crim. Trib. for the Former Yugoslavia Jul. 15, 1999).

a hierarchical structure, a chain of command, and outward symbols of authority to be considered militarily structured groups.[155] If these characteristics existed, then the Russian government could be held responsible under the overall control test, as it applies to militarily structured groups, for the actions of the organized crime groups.[156] However, if organized crimes groups do not qualify as militarily structured groups, it is unlikely that the cyber attackers' actions could be imputed to the Russian state. Here, it is important to differentiate between the organized crime groups and the hacktivists. It would be most difficult to hold the Russian government accountable for the actions of the hacktivists under the overall control test because they were, most likely, not militarily structured, as they are described as volunteers recruited on social networking sites for the purpose of carrying out these specific attacks close to the time of or during the attacks.[157]

Assuming that the organized crime groups in Russia are militarily structured groups, there is a chance that the overall control test may impute responsibility for their actions to the Russian government. A state wields overall control over a militarily structured group by equipping, financing, and coordinating or helping in the general planning of the group's military activities.[158] It is not necessary for the state to issue instructions regarding the group's internationally wrongful actions under the overall control test.[159]

However, given the available facts, it is unlikely that the overall control test applies to the Russian organized crime groups. There is evidence that, prior to August 2008, at least one of the organized crime groups involved in the conflict used and leased botnets similar to the ones used in the cyber attacks.[160] While it may be assumed that the Russian government informed the organized crime groups of its plans to wage a kinetic attack against Georgia, this alone would be insufficient to assign responsibility for the cyber attacks to the Russian government unless those communications constituted coordinating or helping in the general planning of the groups' military activities. Even then, in order to satisfy the test, the Russian government would have also needed to equip and finance a group that was already equipped and already financed.

Conversely, if the organized crime groups in Russia are not

---

[155] *Id.*
[156] *Id.*
[157] U.S. Cyber Consequences Unit Special Report, *supra* note 23, at 2-3.
[158] Tadić, *supra* note 88, ¶ 131.
[159] *Id.* ¶ 131.
[160] Shakarian, *supra* note 15, at 64.

militarily structured groups, they must meet the overall control test's higher bar for activity to impute responsibility to the Russian government.[161] For a state to be held responsible for the actions of its citizens as opposed to its militarily structured groups, the state must have specifically instructed its civilians to conduct unlawful activities or must have formally approved and endorsed those activities.[162] Again, it is unlikely that the Russian state gave specific instructions to its citizens to launch a cyber attack against Georgia. No information has been discovered that would prove such instructions, nor has the Russian government formally approved the cyber attacks. The interactions between the Russian government and the organized crime groups and hacktivists fail to satisfy the requirements of the overall control test.

a. Subsequent Endorsement of Actions

In the Georgia-Russia conflict, Russia did not subsequently authorize the actions of the organized crime groups or of the hacktivists. Similar to what happened in the *United States Diplomatic and Consular Staff in Tehran* case cited above,[163] had Russia subsequently authorized the attacks by claiming that the cyber attackers were acting in defense of the Russian state, it would have implicitly authorized the cyber attacks and then could have been held responsible for the attacks. Article 51 of the UN Charter authorizes only states to use force in self-defense against other states.[164] If Russia subsequently authorized the attacks as a form of self-defense, it would be imputing state power to the cyber attackers. Russia's subsequent claim that its civilians were acting in self-defense would have likely risen to the level of formal approval of the attacks needed to attribute responsibility for the cyber attacks to the Russian government. The closest anyone in the government has come to approving the actions occurred when a low-level official said that the cyber attacks were part of a larger information battle against the West.[165]

The fact that Russia has not subsequently endorsed the citizens' cyber attacks voids Russia's possible claim that the cyber attackers were merely acting in self-defense of their fellow Russians. It would be

---

[161] Tadić, *supra* note 88, ¶ 137.
[162] *Id.* ¶ 132.
[163] *Id.* ¶ 133; *See* Section II.C.
[164] UN Charter, art. 51. While national, regional, and local legal regimes often provide self-defense arguments for criminal and tort offenses, on the international stage, only states may claim self-defense against other state actors.
[165] Shakarian, *supra* note 15, at 64.

disingenuous for Russia to claim that it did not authorize the attacks, yet still claim that its citizens were acting on behalf of the government to defend the Russian civilians in South Ossetia and Abkhazia. Furthermore, there is no incentive for the Russian government to subsequently authorize the cyber attacks. Endorsing the attacks would only lead to responsibility for the attacks being imputed to the Russian government. Under the current regime, the Russian government can enjoy the benefit of the cyber attacks without accepting responsibility for them.

IV. Problems with the Current Attribution Regime and Proposals for a New Regime

Under the current regime for state attribution, the level and type of support given by the state to the non-state actor is scrutinized: the greater and more critical the support, the more likely it is that a state will be held responsible for the actions of a non-state actor.[166] The low-cost of cyber attacks and the ease with which they can be carried out allow the support regime to be reversed. For example, the effective control and overall control tests require the state to provide support to the non-state actor.[167] However, in the Georgia-Russia conflict, the cyber attackers provided important support to the Russian military by disrupting communications and isolating both the Georgian state from the other states and the citizenry from the government. The cyber attackers could have done this without anything more than mere knowledge of when the kinetic attacks were to take place. The organized crime groups already had the means to carry out the attacks. They only needed to mobilize anti-Georgian, Russian-friendly citizens to assist in the attacks' execution. The circumstances of the Georgia-Russia cyber conflict create problems when applying the current attribution tests; therefore, a new test should be devised for state attribution when a cyber attack is involved.

There are differences and similarities between the attribution issues in both *Nicaragua* and *Tadić* and the Georgia-Russia conflict. Most conspicuously, in the most recent conflict, a state was likely working with non-state actors to conduct *a cyber attack* against another state whereas in previous cases states were working with non-state actors to conduct *armed attacks* against another state. Another major difference is that in previous cases, the armed groups were located in the target state, while the cyber

---

[166] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 106 (June 27); Tadić, *supra* note 88, ¶ 120.
[167] *Id.*

attackers were located, in large part, within the state launching the main armed attack. This highlights a major difference between armed groups and cyber groups: a cyber attack group can be located anywhere throughout the world. It does not necessarily have to be located in the target state or in the attacking state. This creates a significant evidentiary problem. Whereas the armed attackers can be found and located in the middle of the conflict, cyber attackers can be located throughout the world. In the Georgia-Russia conflict, it is also important to remember that there were two groups involved: the organized crime groups and the hacktivists, meaning that the parties responsible were not even centrally located within Russia.

Furthermore, hacktivists can make it appear as though a cyber attack is originating in a country other than the one in which it is actually originating.[168] One scholar noted that "[a]nonymity is in fact one of the greatest advantages of cyber warfare: even though the attacks might appear to originate from computers located in a certain country, this does not necessarily mean that that country, or even the owners of the computers involved, were behind such actions."[169] The non-state actors in this case were organized crime groups and civilian hacktivists that could have been launching the attacks from the comfort of their home, business, or neighborhood Internet cafe.

This issue of location of the perpetrators also raises legal questions. In the Georgia-Russia conflict, experts were able to narrow the cyber attackers' location to organized crime groups within Russia and hacktivists mostly located within Russia.[170] This helped narrow the scope of assigning responsibility for the attacks and may prove critical in narrowing responsibility. The ICTY argued that in the case of a state that employs non-state actors to achieve its territorial ambitions over a neighboring state, the bar may be lower than that articulated in the overall control test, meaning it would be easier to attribute the actions of non-state actors to a state if those actions furthered the territorial ambitions of that state.[171] Therefore, if a connection can be shown between the Russian government and the cyber attackers, the bar for attributing responsibility for the attacks to the state may be lower due to Russia's territorial ambitions over Georgia. Russia did not annex South Ossetia or Abkhazia following its incursion into Georgia, which would have been a clear demonstration of Russia's

---

[168] Roscini, *supra* note 129, at 96.
[169] *Id.*
[170] U.S. Cyber Consequences Unit Special Report, *supra* note 23, at 2-3; Shakarian, *supra* note 15, at 64.
[171] Tadić, *supra* note 88, ¶ 140.

territorial aspirations.[172] Instead, Russia remains a protectorate for the two break-off regions.[173]

Another difference, and attribution difficulty, between the court-investigated situations and the Georgia-Russia cyber attacks is that many of the attacks against Georgia were carried out by individual hacktivists, whereas the attacks in *Nicaragua* and *Tadić* were carried out by armed groups. It is easier to define what a group of people has done than it is to determine what many separate individuals have done. While there is some precedent for tribunals holding states liable for individual civilians' actions, it would be extremely difficult for a state to find and prosecute every hacktivist involved in a cyber attack, especially after the attack has occurred. This is due to the number of participants and difficulty in ascertaining the attackers' identity.

Yet another difference between the international tribunals' cases and the Georgia-Russia situation that leads to problems of application of existing attribution law is that of the equipping and financing the cyber attacks. This was a factor that both the ICJ and the ICTY considered important in determining whether or not a state should be responsible for the actions of a non-state actor.[174] One expert estimated the cost of a cyber campaign at "[four] cents per machine" or, in total, "the cost of replacing a tank tread."[175] This low cost and easy access allow small groups and individuals to get involved: "unlike in traditional warfare, cyberspace attacks can easily be carried out not only by states, but also by groups and even individuals: all it takes is a computer, software and a connection to the Internet."[176] In the Georgia-Russia conflict, the Russian government probably did not supply the cyber attackers with botnets, servers, or computers to wage the attacks. In fact, Russian organized crime groups, most notably the Russian Business Network, use and lease the same botnets used in these attacks for their own criminal purposes and most likely provided their own resources for the attack.[177] Determining the location and identity of cyber attackers due to the low cost of cyber attacks and the ability to mask the true origin of the attack are difficulties that do not arise in armed attacks. These differences between cyber and kinetic attacks show the importance of developing a different test for state attribution in

---

[172] *Russia Recognizes Georgia's Breakaway Republics*, RIA NOVOSTI (Aug 26, 2008), http://en.rian.ru/russia/20080826/116291407.html.
[173] *Id.*
[174] Nicaragua, *supra* note 69, ¶ 108; Tadić, *supra* note 88, ¶ 131.
[175] Markoff, *supra* note 18.
[176] Roscini, *supra* at note 129, at 97.
[177] Shakarian, *supra* note 15, at 63.

cases where cyber attacks are used in conjunction with armed attacks.

V. Shifting the Focus to the Timing of Kinetic and Cyber Attacks

One factor that helped narrow the scope of where to attribute responsibility in the Georgia-Russia conflict was the coordinated timing of the kinetic and attacks. This factor may be a good starting point in determining whether a state is responsible for a non-state actor's actions.[178] In the Georgia-Russia conflict, the fact that both attacks happened at essentially the same time led many cyber security experts to believe that the Russian government had at least informed the cyber attackers of their intent to conduct military operations against Georgia.[179] As an example, if a cyber attack was launched by Brazilian cyber attackers at the same time that a kinetic attack was launched by Russia against the same target, it would be at least a starting point for determining that there may have been some sort of an agreement between the Russian government and the Brazilian cyber attackers that rose to the level of the Brazilian cyber attackers acting as the Russian government's agents.

Placing more emphasis on the timing of attacks may be a workable solution in assigning state responsibility: if a state's kinetic operation against another state is accompanied by a non-state actor's cyber attack, then perhaps the attacking state should be responsible for both attacks. This is certainly not a perfect solution. It is possible that enemies of the state engaging in the armed attack could exploit this option by simultaneously launching a cyber attack, leading to an inaccurate assignment of responsibility.

Nonetheless, a focus on timing should be further explored. It may not rise to the same level as either control test, but perhaps the lower standard of a "working in tandem" test would be sufficient to discourage states from working with non-state actors in carrying out cyber attacks against another state, because the first state could potentially be held accountable for any cyber attack that occurred in tandem with its kinetic attack. The attacking state would then have the burden of proving that it did not work in tandem with the non-state cyber attacker. This solution, of course, fails to include conflicts that are carried out completely in cyber space with no kinetic counterpart that still have devastating effects on the victim state. It may, however, provide a practical solution in dealing with the situation of a cyber attack being carried out in concert with a kinetic

---

[178] Roscini, *supra* at note 129, at 97.
[179] U.S. Cyber Consequences Unit Special Report, *supra* note 23, at 3; Shakarian, *supra* note 15, at 66.

attack.

Conclusion

The increasing prevalence of non-state actors in internal and international armed conflicts continues to raise problems for the international community. Myriad legal questions arise when non-state actors become involved in armed conflicts. These legal questions increase when the non-state actors are the perpetrators of a cyber attack, especially when the cyber attack is conducted in concert with a kinetic attack.

The international community should apprise itself of the attribution issues that arise in a cyber conflict, especially when the cyber attacks accompany kinetic attacks. The tests articulated in *Nicaragua* and *Tadić* do not provide a strong solution for cyber conflict. Article 8 of the Draft Articles on State Responsibility was written in light of the *Nicaragua* and *Tadić* tests and draws heavily on the analysis of those two cases. It also fails to grasp the scope of the problem of attribution for cyber attacks.

States should consider the difficulty in identifying the host-state of a cyber attack because of the attendant difficulty in determining the initiator and perpetrator of cyber attacks when developing a new rule of state responsibility. States should also look to differences between the non-state participants in kinetic warfare and cyber warfare, as well as the relative ease at which cyber warfare can be financed and the means to launch a cyber attack can be made accessible. The international community should develop a new test for determining how much control a state needs to exercise over a non-state actor in a kinetic conflict in order to attribute responsibility for the non-state actor's actions to the state. At least one factor in this test should be the temporal proximity within which the kinetic attack occurred and when the cyber attack took place. This factor is not a perfect approach: cyber attackers unfriendly to the state launching armed attacks may take advantage of the test in order to assign blame for the cyber attacks to the state that is launching the armed attack. However, it may be a good starting point in thinking about attribution issues when cyber attacks and armed attacks are carried out together.