Brigham Young University International Law & Management Review

Volume 11 | Issue 2 Article 4

8-1-2015

Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture

Trevor McDougal

ESTABLISHING RUSSIA'S RESPONSIBILITY FOR CYBER-CRIME BASED ON ITS HACKER CULTURE

Trevor McDougal[*]

I. INTRODUCTION

Russia has established a lackadaisical approach to both intellectual property rights and cyber-crime enforcement, particularly the relatively open nature of markets that sell unlicensed copies of software, movies, and music within the country[1] as well as the spread of cyber-crime seemingly originating from within the Russian Federation that causes harm in other nations,[2] including the data breach at Target in 2013.[3] These issues call into question the legal obligations Russia has in preventing its citizens from causing disruptions outside its borders or in limiting the damages they cause. These obligations are often complicated

[*] Juris Doctor candidate, 2016, Brigham Young University, Provo, Utah.

[1] *See* Ryan O'Connell, *MPAA Names Top Online Sites Pirating Movies – Russia, You're First*, THEWRAP: COVERING HOLLYWOOD (Oct. 27, 2014, 11:05 AM), http://news.yahoo.com/mpaa-names-top-online-sites-pirating-movies-russia-150500636.html (noting that the MPAA has identified Russian sites—both direct download and peer to peer—as being the worst online offenders); Erik Gruenwedel, *MPAA Reveals "World's Most Notorious" DVD Piracy Markets*, HOME MEDIA MAGAZINE (Oct. 27, 2014), http://www.homemediamagazine.com/piracy/mpaa-reveals-worlds-most-notorious-dvd-piracy-markets-34466 (describing the Motion Picture Association of America's listing of the worst physical distributors of pirated content, which included physical markets such as Mutino Market in Moscow where titles can be made to order, allowing a purchaser to select a movie after which the DVD is created on nearby premises).

[2] *See* Lukas I. Alpert, *Cyber Attack Thought to Originate in Russia*, WALL ST. J. DIGITS BLOG (Mar. 28, 2013, 7:36 PM), http://blogs.wsj.com/digits/2013/03/28/cyber-attack-thought-to-originate-in-russia/ (noting that an attack targeting a spam-fighting group "appears to have been launched by a gang of hackers from Russia"); Larry Barrett, *Russia, Brazil Lead Cyber Attack Barrage*, ESECURITYPLANET (Jan. 15, 2010), http://www.esecurityplanet.com/trends/article.php/3858971/Russia-Brazil-Lead-Cyber-Attack-Barrage.htm (noting that more cyber attacks originated from Russia than from any other country during the third quarter of 2009); Jessica Guynn & Kevin Johnson, *Is Russia Tied to JPMorgan Hacking?*, USA TODAY (Aug. 28, 2014, 4:03 PM), http://www.usatoday.com/story/tech/2014/08/28/russia-jpmorgan-hacking-attack/14735649/ (questioning whether Russia is tied to a JPMorgan hacking incident in retaliation for the sanctions imposed against Russia); Ionut Ilascu, *United States Targeted by Cyber Attacks Originating from China, the US, India, and Russia*, SOFTPEDIA (Aug. 25, 2014, 09:51 AM), http://news.softpedia.com/news/United-States-Targeted-by-Cyber-Attacks-Originating-from-China-the-US-India-and-Russia-456235.shtml (noting that between April and September 2013, nine percent of the machines involved in cyber attacks against the United States and forty percent of the machines involved in cyber attacks against Europe were located in Russia, but that "this does not mean that the attackers were in [Russia], only that they used systems in this country"); Nicole Perlroth, *Online Security Experts Link More Breaches to Russian Government*, N.Y. TIMES (Oct. 28, 2014), http://www.nytimes.com/2014/10/29/technology/russian-government-linked-to-more-cybersecurity-breaches.html?_r=0 (noting that while security experts link attacks to the government, there is no direct evidence of involvement).

[3] *See* Andrew Webster, *Massive Target Data Breach May Have Been Caused by a Russian Teenager*, THE VERGE (Jan. 18, 2014, 12:59 PM), http://www.theverge.com/2014/1/18/5322276/target-data-breach-malware-author (noting that the data breach "may have been caused" by a Russian national); *Home Depot Confirms Data Breach, Hit by Same Malware as Target*, RT.COM (Sept. 9, 2014, 10:12 AM), http://rt.com/usa/186224-home-depot-data-breach/ (noting the presence of Russian words inside the code for the virus).

by the circuitous path from the creator of a potential attack to the actual perpetrators of that attack, and then ultimately to the victims of the attack.[4]

In addition to the question concerning the degree of control necessary to attribute the actions of groups within a State to the State itself, other questions loom in the background—does a State have any obligation to control the actions of its private citizens that act outside of its design or even contrary to its wishes? That is, even if a State is not actively helping its citizens perpetrate cyber attacks, does it have an obligation to prevent them from doing so? Can a State be held responsible for not taking sufficient steps to prevent its citizens from attacking governments or businesses in other countries? Because of Russia's history of tacit acceptance of hackers and its lack of enforcement of its own laws against citizens when they cause damage outside the State, Russia should be held responsible for the actions of private citizens acting within its borders when those citizens engage in attacks that have an impact outside of the its boundaries.

Part II of this Comment examines the historical development of a hacker culture in Russia. In this culture, domestic violations of intellectual property rights are rarely enforced and hacking of international groups is rarely punished. Part II analyzes how the government's lack of enforcement has led to a culture that is very open to both pirating and engaging in cyber-attacks. Part III reviews a variety of attacks purportedly made by Russian citizens, possibly with the assistance of the government. It also details some of the difficulties in linking the attacks to the Russian government. Part IV describes the current state of attribution and responsibility for actions of both groups and individuals. Part V applies those principles to past cyber-attacks and potential future attacks, describing why Russia can and should be held responsible for the attacks.

II. THE GROWTH OF A PERVASIVE PIRATING AND HACKING CULTURE

Prior to discussing the attacks purportedly undertaken by Russian citizens, possibly with the complicity of the Russian government, it is useful to understand the historical attitudes Russia and its citizens have taken with respect to technology, intellectual property enforcement, and hacking and the ultimate establishment of a culture that is conducive to, and even supportive of, hacking.

A. Legal Situation

Legally, intellectual property has a basis in the Constitution of the Russian Federation: "Each [person] is guaranteed the freedom of literary, artistic, scientific, technical, and other forms of creation, and teaching.

[4] *See* Alpert, *supra* note 2. Despite investigations into the attacks, reports can only state that attacks "appear" to, "may," or "are believed to" have originated from Russia or that machines in a specific country were used in an attack but may have been controlled by users in another country.

Intellectual property is protected by the law."[5] To protect intellectual property, Russia has established a variety of federal services that perform functions similar to the United States Patent and Trademark Office and Copyright Office. In particular, Rospatent "is a Federal executive authority performing functions of control and supervision in the area of the legal protection and exploitation of intellectual property rights, including patents and trademarks."[6] The Russian Civil Code provides a variety of standard protections to the holders of various intellectual property forms (copyrights, patents, trademarks, trade secrets) including the right to exclude others from using that intellectual property, reimbursement for damages against those who have infringed on those rights, and seizure of infringing articles.[7]

In addition, the Russian Criminal Code imposes liability on violators of copyright, patent, and trademark rights.[8] The Criminal Code provides for penalties of 200,000 rubles or an amount in accordance with the income of the offender. Other potential penalties include forced labor for 480 hours, correctional labor for one year, or arrest for six months if the holder of the right suffered "serious injury."[9] Despite the legal foundation for intellectual property, the citizenry at large is often in violation of various forms of intellectual property.[10]

In the realm of hacking and cyber-crime, Russia similarly has criminal provisions preventing unauthorized access to computer information, preventing the creation, use, and spread of harmful computer programs, and preventing the inappropriate use of computer and telecommunication networks.[11] The penalties for creating harmful programs are even more severe than for infringement of intellectual property—up to four years of prison or forced labor.[12]

---

[5] KONSTITUTSIIA ROSSIISKOI FEDERATSII [KONST. RF] [CONSTITUTION] art. 44(1) (Russ.) (translation by the author, emphasis added).

[6] *About Rospatent*, FEDERAL SERVICE FOR INTELLECTUAL PROPERTY (ROSPATENT) (Nov. 2, 2012, 12:21), http://www.rupto.ru/rupto/portal/7bea6e78-fbd2-11e0-e807-8e000200001f?lang=en.

[7] GRAZHDANSKII KODEKS ROSSIISKOI FEDERATSII [GK RF] [Civil Code] art. 1225–1551 (Russ.), *available at* http://www.rupto.ru/rupto/nfile/3b05468f-4b25-11e1-36f8-9c8e9921fb2c/Civil_Code.pdf (unofficial translation by Rospatent).

[8] UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] art. 146–47, 180 (Russ.).

[9] *Id.* at art. 146 (translation by the author). The penalties for violating patent rights are similar. *Id.* at art. 147.

[10] *See Russian Federation: 2014 Special 301 Report on Copyright Protection and Enforcement*, INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE 61 (2014), *available at* http://www.iipa.com/rbc/2014/2014SPEC301RUSSIA.PDF (noting that "VKontakte, the most popular online social network in Russia . . . is the largest single distributor of infringing music in Russia, and also is a hotbed for online piracy of movies," that "Russian IP addresses accounted for more than 36% of the global volume of detected infringements occurring on public peer-to-peer networks," and that "pre-release DVDs of major film titles often appear on the Internet (and then in pirate hard copies sold online or in markets), within a few days after the authorized theatrical release"). In addition, Russia is still on the International Intellectual Property Alliance Priority Watch list several years after acceding to the WTO. Press Release, International Intellectual Property Alliance, IIPA Urges Government Action to Reduce Copyright Piracy, Open Markets, and Protect Creators 1 (Feb. 7, 2014), *available at* http://www.iipa.com/pdf/2014_Feb07_SPEC301_PRESS_RELEASE.pdf.

[11] UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] art. 272–74 (Russ.).

[12] *Id.* at art. 273.

B. Actual Situation

As demonstrated above, the problem is not a lack of appropriate legislation. Rather, the main issue relates to jurisprudential practices and the lack of enforcement by authorities.[13] This lack of enforcement is particularly visible when looking at the accessibility of counterfeit or pirated goods in Russia. Despite some indication of efforts on the part of governmental authorities, counterfeit goods are readily available in Russia.[14] Fines are low when compared to other nations, liability is often not imposed on infringers, and police officers frequently are hesitant to initiate prosecution against the creators and distributors of counterfeit goods.[15] For the over 1,300 raids conducted in 2004 targeting music pirates, an average penalty of fifty dollars was assessed—far too little to have any punitive or deterrent effect.[16] While criminal penalties are available for violators of intellectual property rights, civil or administrative penalties are far more likely to be employed against the perpetrators.[17]

There have been attempts to purge illegal content from Russian websites; however, these efforts have been ineffective thus far.[18] Sites distributing pirated music, movies, and software are rampant in the Russian Internet system, with seemingly little effort taken to stop them.[19]

The same facets that attract many technology businesses to Russia may also be leading to the development of harmful elements among the population. Google, Microsoft, and other companies seek out Russian programmers because of their high skills and relatively low wage level.[20] The Soviet Union was known for its strength in both math and science, and this tradition continues with Russia's current educational system.[21] However, Soviet education was not limited to traditional subjects: having lived through chronic shortages, citizens developed strategies for survival that "included building networks, manipulating systems, [and]

---

[13] *Russian Federation: 2014 Special 301 Report*, *supra* note 10 (noting a decline in the number of raids in 2013 versus prior years and the general preference of the Russian authorities to go after physical markets instead of online markets).

[14] *Intellectual Property Enforcement in Russia and the Ukraine*, CMS CAMERON MCKENNA 12 (2013), http://www.cms-cmck.com/Hubbard.FileSystem/files/Publication/fa6e7d45-a045-41f4-a52f-baf7700885fb/Presentation/PublicationAttachment/0b4352e7-acff-4a21-a718-f0d5e2dd0fd2/(S)%201305-000055%20(V4)%20BROC%20Intellectual%20Property%20Enforcement%20in%20Russia%20and%20the%20Ukrain.pdf.

[15] *Id.*

[16] Candace S. Friel, *The High Cost of Global Intellectual Property Theft: An Analysis of Current Trends, the TRIPS Agreement, and Future Approaches to Combat the Problem*, 7 WAKE FOREST INTELL. PROP. L.J. 209, 226 (2006).

[17] Esprit Eugster, *Evolution and Enforcement of Intellectual Property Law in Russia*, 9 WASH. U. GLOBAL STUD. L. REV. 131, 147 (2010).

[18] Nikolas K. Gvosdev, *The Bear Goes Digital: Russian and Its Cyber Capabilities*, *in* CYBERSPACE AND NATIONAL SECURITY: THREATS, OPPORTUNITIES, AND POWER IN A VIRTUAL WORLD 173, 179 (Derek S. Reveron, ed., 2012) ("Yuri Milner, the CEO of Digital Sky Technologies (who sits on the presidential commission tasked with overseeing Russia's economic modernization) has been asked to look at ways that 'illegal content' could be purged from RUNET sites—a legitimate effort certainly to deal with copyright violations. . . .").

[19] O'Connell, *supra* note 1.

[20] CMS CAMERON MCKENNA, *supra* note 14, at 4.

[21] Clifford J. Levy, *What's Russian for "Hacker"?*, N.Y. TIMES WEEK IN REVIEW (Oct. 21, 2007), http://www.nytimes.com/2007/10/21/weekinreview/21levy.html?pagewanted=all.

solving problems by any means available."[22] It would seem that this history has helped lead to the belief that if an individual can do or gain something (by using computer skills or intelligence), the individual has earned what is obtained. Furthermore, the rampant corruption in Russia has likely led the average citizen to view adherence to the law as generally unnecessary—if the authorities do not need to obey the law, why should an average citizen?[23] Western restrictions on technology transfers in the 1970s and 1980s also likely contributed to the current situation: computer specialists were forced to "disassembl[e], examin[e] and hack[] American systems to see how they worked in order to make them functional on Soviet systems."[24]

After the collapse of the Soviet Union, there were simply not enough jobs in the former Soviet bloc for the computer talent that existed.[25] With the end of the Soviet Union, large groups of talented high school and university students had a choice: enter the legitimate job market for salaries far below their skill level or seek much more lucrative offers available by hacking or working for criminal organizations.[26] Indeed, hacking is not just a potential job, it is "one of the few good jobs left."[27] This has led Russians to view hacking as a positive position: hackers are "fighters for [I]nternet freedom" and "high[ly] skilled programmer[s]."[28]

Russia's late entry into the Internet era along with a culture that is comparatively more xenophobic than others has led to the relatively self-contained nature of the Russian Internet. "Russians tend to communicate with Russians in Russian about Russia-related topics. . . . The Russian blogosphere is, for the most part, an inwardly-focused social network."[29] Russians have a tendency to use Russian sites instead of Western brands such as Google or Facebook.[30] Furthermore, government-friendly businesses own majorities in many of Russia's most popular sites, including its social networking sites, to ensure that the government has access to and control over the majority of data generated in the country.[31] There seems to be an implied agreement between the Russian government and large Russian cybercriminals: 1) do not touch anything within Russia; 2) share anything you find that is of interest to the Russian government; 3) participate whenever Russia needs you for "patriotic activities."[32] As long as Russian cybercriminals follow these three rules, they maintain an "untouchable status."[33]

---

[22] Joseph D Serio & Alexander Gorkin, *Changing Lenses: Striving for Sharper Focus on the Nature of the "Russian Mafia" and its Impact on the Computer Realm*, INT'L REV. L. COMPUTERS & TECH. 191, 192 (2003).

[23] Levy, *supra* note 21.

[24] Serio & Gorkin, *supra* note 22, at 193.

[25] *Id.*

[26] Xinyuan Wang & Daniel Rasbrock, *Chapter 8: The Botnet Problem*, *in* NETWORK AND SYSTEM SECURITY 119, 123 (John A. Vacca ed., 2010).

[27] Serio & Gorkin, *supra* note 22, at 193 (quoting a Russian hacker).

[28] Roman Dremliugal, *Subculture of Hackers in Russia*, 10 ASIAN SOC, SCI. 158, 160 (2014).

[29] Gvosdev, *supra* note 18, at 174.

[30] *Id.*

[31] *Id.* at 179.

[32] Perlroth, *supra* note 2 (quoting Tom Kellerman, Chief Cybersecurity Officer at Trend Micro).

[33] *Id.* (quoting Tom Kellerman).

Evidence seems to suggest that law enforcement actions are taken against hackers after they target *Russian* institutions—there is no haste in prosecuting those who are attack the West.[34] In addition, those who are arrested for hacking seem to be offered jobs working for the Federal Security Service (FSB) instead of being sent to prison.[35] Indeed, the situation might "worsen as hacking, cracking[,] and virus writing shift from being a mischievous hobby of young kids to a lucrative occupation of skilled professionals working hand-in-hand with hardened criminals."[36] While those in the past viewed hacking as a noble endeavor, attempting to bring Western programs to the masses for free, modern Russians are more driven by the lack of adequate jobs.[37] Hacking magazines and software are sold on the streets, and there are plenty of students who excel at mathematics, computer science, and physics who are unable to find jobs.[38] As recently as November 2013, the magazine "Hacker" was released with a DVD that contained computer programs that can crack passwords.[39]

Part of the problem is the fact that, while hacking is illegal in Russia, it is not viewed as morally wrong.[40] While Russians do not balk at the issuance of "Hacker," they would likely not tolerate a magazine aimed at more physical crimes like burgling.[41] Hackers are criminals only because of the legal prohibitions against it, not because of any moral opprobrium.[42]

Perhaps connected to this, authorities do not pursue investigations into cyber-crime to the same extent as other crimes that are deemed higher priorities, particularly when the hacking has not been directed at Russian companies or organizations.[43] These hackers provide their services for a fee, using various sites to find willing buyers.[44] The fact that hackers can use known websites and provide their services with little to no interference from federal authorities is troubling, to say the least.[45] Youth movements, with ties to the government, provide a network of hackers that target those who are viewed as opponents of Russia,

[34] Gvosdev, *supra* note 18, at 180–81.

[35] *Id.* at 181.

[36] John Blau, *Russia – A Happy Haven for Hackers*, COMPUTER WEEKLY (last visited Sept. 17, 2015), http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers.

[37] *Id.*

[38] *Id.*

[39] Dremliugal, *supra* note 28, at 160.

[40] Blau, *supra* note 36.

[41] Dremliugal, *supra* note 28, at 160.

[42] *Id.*

[43] Blau, *supra* note 36. In addition, Russian courts often choose lighter sentences when actions are taken against hackers, even when more harsh sentences are available. Dremliugal, *supra* note 28, at 160 (noting the light sentence for a cyber criminal who targeted the Russian airline Aeroflot).

[44] Max Goncharov, *Trend Micro Incorporated Research Paper 2012: Russian Underground 101*, TREND MICRO (2012), *available at* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf. Hackers offer to combine executable files with PDF files resulting in toxic files ($420), denial of service attacks ($10 per hour, $1,200 per month), botnets ($200 for 2,000 bots), social engineering services (i.e. non-software methods of gaining access to protected information), and account hacking, among many other services. *Id.*

[45] In assembling the data in the report, Trend Micro went to "online forums and services used by Russian cybercriminals" and "relied on articles written by hackers on their activities, the computer threats they create, and the kind of information they post on forums' shopping sites." *Id.* at 1.

enabling the government to deny involvement.[46] And because Russian hackers are often, in some aspects, *better* than their Western peers, the government has not seen the need to shut down one of its best weapons against the West.[47] As long as hackers do not target organizations inside the country and participate in government-sponsored campaigns when asked, the government sees no reason to shut them down.[48]

III. LINKING RUSSIA AND RUSSIANS TO PAST CYBER-CRIMES

A. Estonia in 2007

In 2007, a feud erupted between Estonia and Russia over the removal of a Soviet war monument from the center of Tallinn to a military cemetery.[49] In the following weeks, rioting and looting by thousands of ethnic Russians ensued, which Estonia purported was orchestrated by Russia.[50] In Russia, Estonia's embassy was attacked.[51] Amidst all of the physical violence and confrontations, a cyber battle was raging against both Estonia's State websites and private sites: a series of "denial of service" attacks rendered the sites inoperable.[52] Sites that averaged one thousand visits per day received two thousand hits per second.[53] Some of the attacks defaced Estonian websites, adding Russian propaganda or bogus apologies to the sites.[54] The attacks lasted approximately three weeks, during which Estonia requested that Russia help stop the attacks to no avail.[55] Finally, Estonia reached out to NATO allies for assistance.[56]

The financial losses alone from the relatively simple attacks were quite staggering, with some estimating the total at 750 million euros.[57] While Estonia claimed that some of the earliest attacks came from computers with ties to the Russian government, most of the attacks came from ordinary computers throughout the world.[58] Instructions on how to

---

[46] Gvosdev, *supra* note 18, at 181–82.

[47] Antone Gonsalves, *Why Russian Hackers Are Beating Us*, CSO ONLINE (Aug. 28, 2014, 7:01 PM), http://www.csoonline.com/article/2600212/data-protection/why-russian-hackers-are-beating-us.html#tk.rss_news?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=information_security%20 (describing how Russians strategically think several moves ahead both defensively and offensively and how the government views underground hacking as a national resource). The Russian marketplace for hacking services has been described as the "true Silicon Valley of the East," providing the "greatest expertise when it comes to ethical hacking, penetration testing[,] and black-hat hacking." *Id.*

[48] *Id. See also* Blau, *supra* note 36 (discussing a penalty, albeit a light one, for a criminal who targeted Aeroflot).

[49] David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber Espionage*, 22 MINN. J. INT'L L. 347, 349–50 (2013).

[50] *Estonia and Russia: A Cyber-Riot*, THE ECONOMIST 42 (May 12, 2007).

[51] *Id.*

[52] Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 5 (2009).

[53] Christopher Rhoads, *Cyber Attack Vexes Estonia, Poses Debate*, WALL ST. J. (May 18, 2007, 12:01 AM), http://online.wsj.com/articles/SB117944513189906904.

[54] *Estonia and Russia*, *supra* note 50.

[55] Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 897–98 (2012).

[56] Sklerov, *supra* note 52, at 5.

[57] Gvosdev, *supra* note 18, at 183.

[58] *Estonia and Russia*, *supra* note 50.

perform a "denial of service" attack spread on Russian-language Internet sites.[59] Of course, any attempt to link the attacks to the Russian government is significantly complicated because of the use of "botnets"—computers that have been infected by a virus and take part in the attacks without the owner of the computer knowing.[60] Articles at the time noted the lack of appropriate recourse for such targeted attacks.[61] Even if there were a proper recourse, there is little evidence to prove that the Russian government was behind the attacks. IP addresses can be cloned and "botnets" can be used, making it difficult, if not impossible, to determine whether or not the Russian government was involved in the attacks.[62]

In the aftermath of the attacks, Russia refused to assist Estonia in tracking down the attackers.[63] They refused to investigate the incident at all.[64] Two years after the attacks, a leader from a pro-Kremlin youth group, Nashi, claimed that the youth group had orchestrated the cyber attacks.[65] While Nashi appears to be well-supported among Russian youth, there are also allegations that the Kremlin pays people to attend protests and rallies.[66] In addition, emails have been revealed which purport that Nashi has been used as a tool for pro-Putin propaganda.[67]

B. South Ossetia in 2008

In August 2008, Russia invaded Georgia to expel its forces from South Ossetia.[68] This was the first large-scale cyber attack conducted parallel to traditional military operations.[69] The cyber attacks isolated Georgia from the outside world and had significant informational and psychological impacts. For example, Georgia was not able to communicate information to its citizens during the conflict.[70] The initial attacks targeted news and government websites, starting just shortly before the commencement of the physical altercations, seemingly indicating that the attackers were involved with the government or at least had obtained reliable inside information about the date of the planned attack beforehand.[71] Similar to the attacks against Estonia, the initial attacks against Georgia were denial of service attacks carried out

[59] *Id.*
[60] *Id.*
[61] *See, e.g.*, Binoy Kampmark, *Cyber Warfare Between Estonia and Russia*, CONTEMP. REV. 288 (Autumn 2007) ("International law remains silent, caught off guard in the face of such technological onslaughts. International aggression, for one, remains a state-centred concept, despite the challenges mounted by the terrorist fascination of GWOT . . . . 'Aggression', reads one UN General Assembly resolution, 'is the use of armed force by a State against . . . another State . . . .").
[62] Wang & Rasbrock, *supra* note 26, at 119.
[63] Sklerov, *supra* note 52, at 10.
[64] Lotrionte, *supra* note 55, at 897–98.
[65] PAULO SHAKARIAN, JANA SHAKARIAN & ANDREW RUEF, INTRODUCTION TO CYBER-WARFARE: A MULTIDISCIPLINARY APPROACH 19 (2013). Nashi was also named as the culprit in the attacks in a top-secret 2009 NSA report. Perlroth, *supra* note 2.
[66] SHAKARIAN ET AL., *supra* note 65, at 19.
[67] *Id.*
[68] Lotrionte, *supra* note 55, at 898.
[69] SHAKARIAN ET AL., *supra* note 65, at 24.
[70] Sklerov, *supra* note 52, at 5.
[71] *Id.* at 4–5.

through botnets.[72] The particular botnets used against Georgian websites were affiliated with criminal organizations in Russia, including the Russian Business Network.[73]

The second phase of the attacks broadened the targets. Instead of just attacking media and government sites, the hackers also targeted financial institutions, businesses, education institutions, and Western media companies. The strategy involved defacement of websites in addition to the denial of service attacks.[74] The second phase also involved recruiting Russian computer users—hacktivists—especially those who were members of youth movements, including Nashi.[75] Many websites, including StopGeorgia.ru, provided instructions on launching denial of service attacks that were accessible even to novice users.[76] These websites were well policed by administrators, limiting access to U.S.-based security scans and removing references to military operations.[77] Despite Georgian attempts to limit Russian attacks by filtering IP addresses, the attackers hid or spoofed their IP addresses and continued their attacks.[78]

After the conflict in Georgia, one Russian individual described how he became a "cyber warrior" by following some steps on different blog sites:

> In less than an hour, I had become an Internet soldier. I didn't receive any calls from Kremlin operatives . . . . My experiment also might shed some light on why the recent cyberwar has been so hard to pin down and why no group in particular has claimed responsibility. . . . [W]e risk underestimating the great patriotic rage of many ordinary Russians, who, having been fed too much government propaganda in the last few days, are convinced that they need to crash Georgian Web sites. Many Russians undoubtedly went online to learn how to make mischief, as I did. Within an hour, they, too, could become cyberwarriors.[79]

While there are certainly official cyber units in Russia, handshake arrangements or other secretive relationships between the government and hackers provide a way for the government to plausibly deny the allegations that it is engaging in cyber warfare.[80] The fact that there was apparently a detailed cyber attack plan in place, ready to go into action, would seem to indicate that the hackers' efforts were "probably

[72] SHAKARIAN ET AL., *supra* note 65, at 24.
[73] GREYLOGIC, PROJECT GREY GOOSE PHASE II REPORT: THE EVOLVING STATE OF CYBER WARFARE 4 (2009), *available at* http://www.fserror.com/pdf/GreyGoose2.pdf.
[74] SHAKARIAN ET AL., *supra* note 65, at 24.
[75] GREYLOGIC, *supra* note 73, at 4–5.
[76] SHAKARIAN ET AL., *supra* note 65, at 25.
[77] *Id.* at 26.
[78] *Id.*
[79] Gvosdev, *supra* note 18, at 182.
[80] GREYLOGIC, *supra* note 73, at 4.

coordinated . . . with the Russian military even if no conclusive evidence exists of such collaboration."[81]

Despite significant research by the Grey Goose project and the U.S. Cyber Consequences Unit, there is no conclusive evidence that links the Russian government to the cyber-attacks launched against Estonia or Georgia.[82] Despite the lack of conclusive evidence, there is some heft to the idea that the government was involved.

C. Target in 2013

From late November through the middle of December 2013, the U.S. retail chain Target was the victim of a hack that compromised the data of millions of customers, including information of forty million credit and debit card accounts.[83] Soon after the breach, the data was available on the black market.[84] All told, personal data for up to seventy million customers were taken in the attack.[85] Target and its partners lost more than two hundred million dollars as a consequence of the breach.[86]

The attack was not limited to Target, however. The same virus used in the Target attack also reached over one thousand other U.S. businesses.[87] More recently, Home Depot suffered a similar attack dating from approximately April 2014 until September 2014.[88] Similar to the previous attacks in Estonia and Georgia, there is nothing to link the Russian government to these attacks. But unlike the prior two incidents, there is little political incentive for Russia to go after retailers in the United States.

Still, there is some evidence that a teenage Russian hacker created the malware that caused the security breach in these cases.[89] While he did not actually attack the department stores, he purportedly wrote the software that was eventually sold to the cyber attackers.[90] The malware was offered for sale for approximately two thousand dollars, with discounts offered to those who agreed to share any profits made by using

[81] Gvosdev, *supra* note 18, at 183.

[82] GREYLOGIC, *supra* note 73.

[83] Chris Welch, *Target Hacked: News and Updates on the Massive Retail Breach That Affected Millions*, THE VERGE (Jan. 16, 2014, 1:42 PM), http://www.theverge.com/2014/1/16/5316006/target-hacked-news-and-updates-on-massive-retail-breach.

[84] *Id.*

[85] *Id.*

[86] Russell Brandom, *Over 1,000 US Businesses Are Affected by the Attack that Hit Target, Says Secret Service*, THE VERGE (Aug. 22, 2014, 3:32 PM), http://www.theverge.com/2014/8/22/6057557/over-1000-us-businesses-are-affected-by-the-attack-that-hit-target/in/5080047.

[87] *Id.*

[88] Adi Robertson, *Home Depot Investigating Potentially Massive Credit Card Hack*, THE VERGE (Sept. 2, 2014, 04:32 PM), http://www.theverge.com/2014/9/2/6098347/home-depot-investigating-potentially-massive-credit-card-hack/in/5080047; Elizabeth Weise, *Home Depot's Credit Cards May Have Been Hacked*, USA TODAY (Sept. 3, 2014, 9:46 AM), http://www.usatoday.com/story/tech/2014/09/02/home-depot-credit-cards-hack-russia-ukraine/14972179/.

[89] Webster, *supra* note 3. *But see Russian Teen Misidentified in Target Breach, Expert Says*, FOX NEWS (Jan. 20, 2014), http://www.foxnews.com/tech/2014/01/20/russian-teen-misidentified-in-target-breach/ (noting that another author crafted the code, but the accused teen still played a role in the breach).

[90] Webster, *supra* note 3.

the software.[91] Part of the malware was written in Russian.[92] In addition, the information that was stolen from Target shoppers was taken from a server in the United States and then sent to a server in Russia.[93] Of course, even the assertions that a Russian citizen created the malware and that the data were eventually sent to Russia does not implicate the Russian government in the attacks for many of the reasons that have been discussed above. Due to the relative ease with which information can be obscured digitally and the fact that the information can be later retrieved from a server in Russia and sent elsewhere, it is impossible to say if the actual attackers were located in Russia.

D. Ongoing Attacks—Energy Companies, Financial Institutions, and More

While not as significant as the attacks against Estonia and Georgia, cyber-attacks happen continually. These attacks generally focus on stealing money from international banks and corporations and personal data from individuals in order to commit fraud.[94] This year alone, Russian hackers have been blamed for attacking oil and gas companies,[95] placing a digital bomb in the NASDAQ,[96] hacking financial institutions,[97] and spying on both the Ukrainian government and a U.S. scholar who specializes in Russian culture.[98] In addition, breaches into the White House computer networks and government computer networks have occurred with some degree of regularity.[99] While most of these events were relatively benign in terms of their effects, the *potential* effects—particularly related to the energy companies—could be quite devastating.[100] The motives in these cases seem to be industrial or

[91] *Russian Teen Believed to Have Developed Software Used in Target Breach*, FOX NEWS (Jan. 19, 2014), http://www.foxnews.com/tech/2014/01/19/russian-teen-believed-to-have-developed-software-used-in-target-breach/.

[92] Webster, *supra* note 3.

[93] Jeremy Kirk, *Target Credit Card Data Was Sent to Server in Russia*, PCWORLD (Jan. 17, 2014, 5:35 AM), http://www.pcworld.com/article/2088920/target-credit-card-data-was-sent-to-server-in-russia.html.

[94] Gvosdev, *supra* note 18, at 183.

[95] Jose Pagliery, *Russia Attacks U.S. Oil and Gas Companies in Massive Hack*, CNN (July 2, 2014, 5:14 PM), http://money.cnn.com/2014/07/02/technology/security/russian-hackers/?iid=EL.

[96] Jose Pagliery, *Russia Hackers Placed 'Digital Bomb' in Nasdaq – report*, CNN (July 17, 2014, 3:49 PM), http://money.cnn.com/2014/07/17/technology/security/nasdaq-hack/?iid=EL.

[97] James O'Toole, *JPMorgan: 76 Million Customers Hacked*, CNN (Oct. 3, 2014, 8:00 AM), http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack/?iid=EL; Matt Egan, *FBI Investigating Hacking Attack on JPMorgan*, CNN (Aug. 29, 2014, 5:41 PM), http://money.cnn.com/2014/08/27/investing/jpmorgan-hack-russia-putin/?iid=EL; Michael Riley & Jordan Robertson, *Russian Hackers Said to Loot Gigabytes of Big Bank Data*, BLOOMBERG (Aug. 28, 2014, 11:46 AM), http://www.bloomberg.com/news/2014-08-28/russian-hackers-said-to-loot-gigabytes-of-big-bank-data.html.

[98] Jose Pagliery, *Russian Hackers Exploit Windows to Spy on West*, CNN (Oct. 14, 2014, 4:09 PM), http://money.cnn.com/2014/10/14/technology/security/russia-hackers/.

[99] Ellen Nakashima, *Hackers Breach Some White House Computers*, WASH. POST (Oct. 28, 2014), http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html (noting that unclassified White House networks had been breached by "hackers thought to be working for the Russian government," at least partially because "the nature of the target is consistent with a state-sponsored campaign" and that such attempts at intrusion happen "on a regular basis").

[100] *See* Nicole Perlroth, *Russian Hackers Targeting Oil and Gas Companies*, N.Y. TIMES (June 30, 2014), http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?_r=0.

corporate espionage, which would be a violation of the rights of the companies for their intellectual property. However, more troubling is that the method used by the hackers "also gives them the opportunity to seize control of industrial control systems from afar."[101] The Russian groups that invaded the energy companies could have used their "toehold in some networks to inflict damage, like blowing up an oil rig or power facility," but there is no evidence that they intended to do that.[102]

In addition to attacks that are focused on shutting down websites, Russian sources, including State intelligence services, have been accused of pursuing hacking activities to steal economic information and technology from targets in the United States, specifically targeting research and development.[103] Russia and China were singled out in a recent report for being "the foreign intelligence services and countries that are doing the most harm."[104] In particular, areas where the U.S. has had a competitive advantage were targeted: pharmaceuticals, aeronautics, and advanced manufacturing techniques.[105] While China is the predominant threat in targeting U.S. intellectual property and trade secrets, Russia is also a significant source of problems.[106]

IV. EXISTING STATE RESPONSIBILITY FOR THE CRIMINAL ACTIONS OF ITS CITIZENS THAT HAVE IMPACTS OUTSIDE OF THE STATE

Given the potentially far ranging and damaging effects of these attacks on outside nations, some important questions need to be asked. What is the duty of Russia with respect to controlling its citizens? Can the attacks be attributed to Russia? Can Russia be held responsible for the actions of its citizens? Attribution and State responsibility are key facets of international law. Without attribution of actions to a State or the responsibility of a State with respect to those actions, nations may be left without adequate recourse.[107] Without a responsible State, a country is left with few options to protect itself from outside threats. Specifically, the State could develop greater defensive capabilities in its own cyber system, strike out against those who are believed to be the attackers, or attempt to reach a diplomatic solution to the problem with the country that is host to the cyber attackers.

However, none of these solutions seems to be an adequate response. Developing effective defenses takes time and resources, and the defenses are often quickly circumvented by continually evolving attacks. Counter-attacks are not likely to deter future threats because of the speed and ease with which the attackers set up new equipment. Finally, current world dynamics do not exert sufficient pressure on countries for them to

[101] *Id.*
[102] *Id.*
[103] Tom Gjelten, *China, Russia Top List of U.S. Economic Cyberspies*, NPR (Nov. 03, 2011, 4:59 PM), http://www.npr.org/2011/11/03/141997331/china-russia-top-list-of-u-s-economic-cyberspies.
[104] *Id.* (quoting a senior intelligence official).
[105] *Id.*
[106] *US to Crack Down on Intellectual Property Theft*, SPUNTIK NEWS (Feb. 21, 2013, 09:58), http://sputniknews.com/voiceofrussia/2013_02_21/US-to-crack-down-on-intellectual-property-theft/.
[107] *See* Statute of the Court of the International Court of Justice, Article 34(1) (noting "only states may be parties in cases before the Court").

regulate attacks originating within their own borders. Some have argued that counting only on passive defense mechanisms, such as anti-virus programs, firewalls, encryption, and automated detection, will lack any significant power of deterrence because such measures do not collect data that can lead to an identification of the perpetrator and thus allows the perpetrator to evade prosecution. In other words, the wrongful acts will continue with impunity.[108]

A. Attribution under the Responsibility of States for Internationally Wrongful Acts

The *Draft articles on the Responsibility of States for Internationally Wrongful Acts* provide thorough understanding of the existing customary international law on attribution of the actions of non-State actors to States.[109] The articles describe the baseline for assessing whether a State should be held responsible for the effects of actions of individuals or groups with ties to the State.[110] There are several ways to attribute conduct to a State. According to the articles, actions by organs of that State, as defined by the internal law of the State, qualify as acts of the State itself.[111] This applies to all levels of government, such as central, provincial, and local, and all branches of government, including legislative, executive, and judicial.[112] Even actions of institutions that are autonomous in a given country but are normally institutions of the government, such as the police force, will be attributed to the State.[113]

In addition, if a person or entity "is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct," the conduct is considered an act of the State.[114] For instance, "when State organs supplement their own action by recruiting or instigating private persons or groups who act as 'auxiliaries' while remaining outside the official structure of the State," the actions of those private persons or groups are attributable to the State.[115] Direction or control presents a more complex issue,[116] as will be discussed below with regard to cases from the International Court of Justice. It "does not extend to conduct which was only incidentally or peripherally associated with an operation."[117] Only one of the three requirements, "instructions," "direction," or "control," must be met, but it must relate to the wrongful conduct.[118]

In addition to the draft articles, international courts have provided insight into what is required for attribution of acts to a State. In

[108] Dimitar Kostadinov, *The Attribution Problem in Cyber Attacks*, INFOSEC INST. (Feb. 1, 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/.
[109] *See Draft articles on the Responsibility of States for Internationally Wrongful Acts*, A/56/10 International Law Commission (2001).
[110] *See id.*
[111] *Id.* at art. 4.
[112] *Id.* at art. 4 cmt. (6).
[113] *Id.* at ch. II cmt. (6).
[114] *Id.* at art. 8.
[115] *Id.* at art. 8 cmt. (2).
[116] *Id.* at art. 8 cmt. (3).
[117] *Id.* at art. 4.
[118] *Id.* at art. 8 cmt. (7).

particular, the International Court of Justice, in its *Nicaragua v. United States* and *Bosnia & Herzegovina v. Serbia & Montenegro* cases, established a framework for analyzing the relationship between the parties and States.

In *Nicaragua v. United States*, the United States was accused of "recruiting, training, arming, equipping, financing, supplying and otherwise encouraging, supporting, aiding, and directing military and paramilitary actions in and against Nicaragua," thus constituting a use of force against Nicaragua with armed attacks.[119] After an initial period of covert operations, official statements by the President of the United States made clear that the U.S. government had been giving support to the *contras*, those who were fighting against the Nicaraguan government.[120] Congressional budgetary legislation "made specific provision for funds to be used by United States intelligence agencies for supporting 'directly or indirectly, military or paramilitary operations in Nicaragua.'"[121] Financing for the military and paramilitary activities of the *contras* was a part of the budget of the United States from 1981 until 1984.[122] The financing was used by the CIA to provide "arms, munitions[,] and military equipment, including uniforms, boots[,] and radio equipment,"[123] along with training in "guerrilla warfare, sabotage, demolitions, and in the use of a variety of weapons" and intelligence regarding Nicaraguan troop movements.[124]

In sum, the support provided by the United States to the *contras* included, at different times, "logistic support, the supply of information on the location and movements of . . . troops, the use of sophisticated methods of communication, the deployment of field broadcasting networks, radar coverage, etc."[125] In addition, several of the military and paramilitary operations "were decided and planned, if not actually by United States advisers, then at least in close collaboration with them, and on the basis of the intelligence and logistic support" which the United States offered.[126] U.S. "authorities largely financed, trained, equipped, armed and organized" the *contras* in their fight with the Nicaraguan government.[127]

Despite the "heavy subsidies and other support provided . . . by the United States," the Court determined that there was "no clear evidence of the United States having actually exercised such a degree of control in all fields as to justify" impugning the actions of the *contras* to the United States.[128] In coming to this conclusion, the Court noted that *contra* activity continued, even after military aid was no longer authorized.[129] Thus, the *contras* could not be said to be in a state of "complete

[119] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 18 ¶ 15 (June 17).
[120] *Id.* at 21 ¶ 20.
[121] *Id.*
[122] *Id.* at 58 ¶ 97.
[123] *Id.* at 59 ¶ 100.
[124] *Id.* at 59 ¶ 101.
[125] *Id.* at 61 ¶ 106.
[126] *Id.*
[127] *Id.* at 62 ¶ 108.
[128] *Id.* at 62 ¶ 109.
[129] *Id.* at 62 ¶ 110.

dependence" on the State.[130] In establishing the degree of control of a State over a non-State group, the selection, installation, and payment of leaders of the group is but one factor.[131] In addition, even given the "financing, organizing, training, supplying[,] and equipping of the *contras*, the selection of its military or paramilitary targets, and the planning of the whole of its operation," not all acts committed by the *contras* could be attributed to the United States—the United States would need to have had "effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[132]

In *Bosnia & Herzegovina v. Serbia & Montenegro*, Bosnia & Herzegovina attempted to attribute the actions of Republika Srpska, namely its army, the Vojska Republike Srpske (VRS) in committing atrocities in the city of Srebrenica to Yugoslavia.[133] "Thousands of men and boys were summarily executed and buried in mass graves within a matter of days" while the international community attempted to gain access to them.[134] The women, children, and elderly people "were uprooted and, in an atmosphere of terror, loaded onto overcrowded buses . . . and transported across the confrontation lines into Bosnian Muslim-held territory."[135] Military-aged men were "taken prisoner, detained in brutal conditions[,] and then executed."[136] There were allegedly close ties between Yugoslavia and Republika Srpska politically and financially; Yugoslavia also allegedly had ties to the administration and control of the VRS.[137] For slightly over ten percent of the officers in the VRS, "payment, promotions, pensions, etc. were handled, not by the Republika Srpska, but by the [Yugoslavian army]."[138] The VRS was also "armed and equipped" by Yugoslavia, with up to ninety percent of its material needs being supplied by Yugoslavia.[139] The Court determined that Yugoslavia "was . . . making its considerable military and financial support available to the Republika Srpska, and had it withdrawn that support, this would have greatly constrained the options that were available to the Republika Srpska authorities."[140]

In evaluating whether the acts were attributable to Yugoslavia, the Court began its analysis with an investigation into the legal recognition of the perpetrators of the action.[141] If the acts were not perpetrated by organs of the State, it needed to determine if they "were committed by persons who, while not organs of the [State], did nevertheless act on the

[130] *Id.* ("In sum, the evidence available to the Court indicates that the various forms of assistance provided to the *contras* by the United States have been crucial to the pursuit of their activities, but it is insufficient to demonstrate their complete dependence on United States aid.").
[131] *Id.* at 63 ¶ 112.
[132] *Id.* at 64–65 ¶ 112.
[133] Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. 43, 64 ¶ 64 (Feb. 26).
[134] *Id.* at 136 ¶ 229.
[135] *Id.* at 155 ¶ 278.
[136] *Id.*
[137] *Id.* at 138–40 ¶ 237.
[138] *Id.* at 140 ¶ 238.
[139] *Id.* at 141 ¶ 239.
[140] *Id.* at 142 ¶ 241.
[141] *Id.* at 201 ¶ 384.

instructions of, or under the direction or control of, the [State]."[142] Organs of a State can be either *de jure* organs, those that hold the status of organ under the internal law of a State,[143] or *de facto* organs, those that "in fact act under such strict control by the State that they must be treated as its organs."[144] Even substantial financial support does not make a group a State organ.[145] Referring back to its *Nicaragua* decision, the Court reiterated that a *de facto* organ is a body over which a State "exercise[s] such a degree of control in all fields" and which is in "complete dependence on [the State's] aid."[146] However, "complete dependence" will not be found often, as "to equate persons or entities with State organs when they do not have that status under internal law must be exceptional, for it requires proof of a particularly great degree of State control over them."[147]

In keeping with this standard, despite the "strong and close" "political, military[,] and logistical relations" between the federal authorities of Yugoslavia and Republika Srpska, they were not of such a degree as to prevent Republika Srpska from acting with "some qualified, but real, margin of independence."[148] In addition, even though the support given by Yugoslavia was such that Republika Srpska "could not have 'conduct[ed] its crucial or most significant military and paramilitary activities'" without it, it was not in a state of "total dependence."[149]

After deciding that VRS was neither a *de jure* nor a *de facto* organ of Yugoslavia, the Court considered whether attribution could be founded on "direction or control."[150] While this may seem similar to the determination of a *de facto* organ of the State, this investigation instead relates to Article 8 of the *Responsibility of States for Internationally Wrongful Acts*.[151] This question does not deal with the general circumstances surrounding the group, but instead whether the State, "in the specific circumstances surrounding [a particular event]" instructed, directed, or controlled the group to perform the actions.[152] Again referring back to its *Nicaragua* case, the Court reiterated that legal responsibility arises if a State is in "effective control of the . . . operations in the course of which the alleged violations were committed."[153] Here, "complete control" is not required, only a State's instructions or its "effective control," which seems to lessen the burden on a plaintiff State.[154] However, the instructions or control must be given "in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons who committed the violations."[155] In reaching its

[142] *Id.*
[143] *Id.* at 202 ¶ 386.
[144] *Id.* at 204 ¶¶ 390–91.
[145] *Id.* at 203 ¶ 388.
[146] *Id.* at 205 ¶ 391.
[147] *Id.* at 205 ¶ 393.
[148] *Id.* at 206 ¶ 394.
[149] *Id.*
[150] *Id.* at 205–06 ¶ 396.
[151] *Id.* at 207–08 ¶ 398
[152] *Id.* at 207 ¶ 397.
[153] *Id.* at 208 ¶ 399.
[154] *Id.* at 208 ¶ 400.
[155] *Id.*

conclusion, the Court specifically rejected the application of the "overall control" test used by the International Criminal Tribunal for the former Yugoslavia (ICTY) in establishing the presence of an international conflict for Yugoslavia with regard to the Republika Srpska and the VRS.[156] Reports after the events in Srebrenica did not suggest that Yugoslavian "leadership was involved in planning the attack or inciting the killing of non-Serbs; nor [was there] any hard evidence of assistance by the Yugoslav army to the armed forces of the Republika Srpska before the attack," thus actions could not be attributed to Yugoslavia.[157]

B. Responsibility to Prevent Damaging Acts under a Duty of Care

State responsibility has primarily developed to limit the responsibility of a State for actions of individual private citizens or groups within its borders.[158] In the comments to the *Draft articles on the Responsibility of States for Internationally Wrongful Acts*, specific mention is made of how all acts linked to the State by nationality, habitual residence, or incorporation could be attributed to the State. However, such an approach was avoided "both with a view to limiting responsibility to conduct which engages the State as an organization, and also so as to recognize the autonomy of persons acting on their own account and not at the instigation of a public authority."[159] "Conduct of private persons is not as such attributable to the State."[160] However, past thought on the matter seemed to be more open to assigning responsibility to a State for actions of individuals: "A state owes at all times a duty to protect other states against injurious acts by individuals from within its jurisdiction."[161] In coming to its conclusion, the commentary on the draft articles cites the *Tellini* case of 1923.[162]

Tellini involved the assassination of Italian members of an international commission while on Greek territory.[163] While Tellini, an Italian, was assisting in the delimitation of the Greece-Albania border, an

[156] *Id.* at 209 ¶ 403. In particular, the Court noted that the ICTY did not "rule on questions of State responsibility, since its jurisdiction is criminal and extends over persons only." *Id.* While the ICJ respected the "factual and legal findings made by the ICTY," it did not feel the need to do so for positions "on issues of general international law which do not lie within the specific purview of [the ICTY's] jurisdiction." *Id.* The Court decided that broadening the scope of State responsibility, which would occur under the "overall control" test, would result in a State being responsible for more than its own conduct. *Id.* at 210 ¶ 406. This tends to "stretch[] too far, almost to breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility." *Id.* The Court's decision not to apply the "overall control" test of *Tadić* and its reasoning have been criticized by some academics. *See, e.g.,* 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 (2007). Furthermore, others argue that, due to the difficulty of proving the identity of cyber attackers, the "overall control" standard of *Tadić* is particularly well suited to issues surrounding cyber-crime. Scott J. Shackelford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, *available at* http://irps.ucsd.edu/assets/001/501281.pdf.

[157] *Bosn. & Herz.*, 2007 I.C.J. 212–13 ¶ 410.

[158] *Id.* at 208 ¶ 400.

[159] *Draft articles on the Responsibility of States for Internationally Wrongful Acts*, *supra* note 111, at ch. II cmt. (2).

[160] *Id.* at ch. II cmt. (3).

[161] CLYDE EAGLETON, THE RESPONSIBILITY OF STATES IN INTERNATIONAL LAW 80 (1928).

[162] *Draft articles on the Responsibility of States for Internationally Wrongful Acts*, *supra* note 111, at ch. II cmt. (3).

[163] *Id.*

unknown party ambushed him and killed him.[164] The International Commission requested redress from Greece because it accused Greece of exercising neglect in pursuing the criminals.[165] The Council of the League of Nations referred the question of Greece's responsibility for the incident to a Special Commission. Specifically, it asked: "In what circumstances and to what extent is the responsibility of a State involved by the commission of a political crime in its territory?"[166] The Commission determined that:

> [T]he responsibility of a State is only involved by the commission in its territory of a political crime against the persons of 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.[167]

The Commission added a caveat to its findings: "The recognized public character of a foreigner and the circumstances in which he is present in its territory entail upon the State a corresponding duty of special vigilance on his behalf."[168] Thus, while the particular facts of the *Tellini* case seem to limit the application of responsibility, it shows that there are times when States could be held responsible for the actions of private individuals within their borders.

Several Court cases have repeated this idea in different contexts. In the *Corfu Channel Case*, the Court was asked to determine whether Albania was responsible for damage caused by mines in its waters.[169] British cruisers and destroyers left the port of Corfu and sailed through the North Corfu Strait.[170] A mine heavily damaged one of the destroyers.[171] When a second destroyer attempted to tow the damaged destroyer to safety, it too struck a mine.[172] Both destroyers returned to Corfu.[173] Investigations revealed that the minefield, located in Albanian territorial waters, had been recently laid.[174] In ascertaining the responsibility of Albania for the damage caused by the mines, the Court determined that Albania need not have taken part in the laying of the mines to nonetheless be responsible.[175]

The Court examined whether Albania knew, or should have known, (given potentially circumstantial evidence) that the mines had been laid.[176] If Albania knew about the mines prior to the incident with

[164] EAGLETON, *supra* note 161, at 187.
[165] *Id.* at 188.
[166] 4 LEAGUE OF NATIONS OFFICIAL J. 1349, 1351 (1923).
[167] 5 LEAGUE OF NATIONS OFFICIAL J. 523, 524 (1924).
[168] *Id.*
[169] Corfu Channel Case (U.K. Gr. Brit. & N. Ir. v. Alb.), 1949 I.C.J. 4, 6 (Apr. 9).
[170] *Id.* at 12.
[171] *Id.* at 12.
[172] *Id.* at 12.
[173] *Id.* at 12–13.
[174] *Id.* at 13.
[175] *Id.* at 17. The Court comes to the conclusion that the fact that the "author of the minelaying remain[s] unknown" is not critical to the determination of whether or not Albania is responsible for the explosions that occurred. *Id.*
[176] *Id.* at 17–22.

sufficient time to warn the British vessels, it would be responsible for the incident.[177] In this case, "the obligations incumbent upon the Albanian authorities consisted in notifying, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in warning the approaching British warships of the imminent danger to which the minefield exposed them."[178] These obligations stem from "general and well-recognized principles, namely: elementary considerations of humanity . . . and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[179] Albania's omission—choosing to remain silent rather than to warn the British ships—thus resulted in its international responsibility for the incident.[180]

More recently, the Court reiterated the obligation of a State to prevent or limit harm to other States in *United States v. Iran*. Similar to the *Corfu Channel Case*, this case does not deal with government action; instead Iran was accused of "tolerating, encouraging, and failing to prevent and punish conduct" that resulted in the United States being unable "to have access to its diplomatic and consular representatives, premises[,] and archives in Iran."[181]

After the United States allowed the former Shah of Iran to enter its territory for medical treatment, large demonstrations took place in Iran, and many demonstrators marched in front of the United States Embassy but did not cause any issues.[182] A few days later, however, an armed group of demonstrators overran the embassy compound with no resistance from the Iranian security personnel.[183] All of the diplomatic and consular personnel were taken hostage and detained in the compound.[184] Despite repeated calls for help, no forces were sent in time to provide protection.[185] The following day, consulates in two other cities were seized without any protective action on the part of the Iranian government.[186]

The militants who attacked the embassy had no official status as organs of the Iranian State and there was not sufficient information before the Court to establish a link between the militants and the State: this was not a case of a *de jure* or *de facto* organ of the State.[187] While the Ayatollah Khomeini had issued several public declarations calling for students "to expand with all their might their attacks against the United States," the declaration was far from State authorization to take the specific actions (invading and occupying the Embassy) that were ultimately taken.[188] Even celebratory phone calls after the event "do not

[177] *Id.* at 22.
[178] *Id.*
[179] *Id.*
[180] *Id.* at 23.
[181] United States Diplomatic & Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, 6 ¶ 8, 9 ¶ 11 (May 24).
[182] *Id.* at 12 ¶¶ 15–16.
[183] *Id.* at 12 ¶ 17.
[184] *Id.*
[185] *Id.* at 12–13 ¶ 18.
[186] *Id.* at 13 ¶ 19.
[187] *Id.* at 29 ¶ 58.
[188] *Id.* at 29–30 ¶ 59.

alter the initially independent and unofficial character of the militants' attack on the embassy."[189] However, despite the fact that the Iranian government was not involved in the initial actions of the militants in seizing the embassies, its lack of action in taking any "appropriate steps" to protect the embassy against attack or to prevent the attack demonstrate "more than mere negligence or lack of appropriate means."[190]

Because Iran was "fully aware of [its] obligations under the conventions in force," because it was "fully aware . . . of the urgent need for action," because it "had the means at [its] disposal to perform [its] obligations," and because it "completely failed to comply with these obligations," it could be held responsible for the results of the actions of the militants.[191] Notably, however, this case deals with obligations arising under the Vienna Conventions,[192] not a customary law to prevent harm to other nations.

It is important to note that these cases developed long before the issuance of the draft articles on State responsibility. The *Iran* case was decided twenty years prior to the articles, which, as mentioned before, seem to downplay the ability of States to be held responsible for the actions of private citizens.[193] However, the principles and the ideas stated are very applicable to the idea of rectifying, and hopefully reducing, the effects of transnational cyber-crime.

V. APPLICATION TO PAST CYBER-CRIME AND POTENTIAL APPLICATION TO FUTURE MISDEEDS

A. Difficulty of Attribution

As discussed above in reference to the various attacks in which Russia has been implicated, no direct evidence of the involvement of a Russian organ in the attacks has ever been found, despite an abundance of circumstantial evidence to that effect.[194] Thus, none of the situations to date (and likely no situation in the future, barring reckless work on the part of official State agencies) can be viewed as the actions of *de jure* organs of Russia.

Attempting to apply the *Nicaragua* standard shows the problems faced by States that are subject to cyber-attacks. Barring significant missteps by the attackers, it will be nearly impossible to meet the high threshold requirement of control that the Court has enunciated—it is simply too difficult to pin down an exact source.[195] Even the process of

[189] *Id.* at 30 ¶ 59.
[190] *Id.* at 31 ¶ 63.
[191] *Id.* at 32–33 ¶ 68.
[192] *Id.* at 37 ¶ 79.
[193] *Draft articles on the Responsibility of States for Internationally Wrongful Acts*, *supra* note 111, at ch. II cmt. (3).
[194] *See supra* Part III.
[195] Jose Pagliery, *It looks like Russia and smells like Russia . . . but is it Russia?*, CNNMONEY (Oct. 31, 2014 8:41 AM), http://money.cnn.com/2014/10/31/technology/security/russia-hackers/ (noting that when attacks are attributed to the Russian government, circumstantial evidence is used: the virus was written in Russian, created during Moscow working hours, and aimed at anti-Russian targets). In addition, cyber spies from the United States, the United Kingdom, France, Israel, and Russia are "known to leave decoys that make attacks appear to come from elsewhere," further obfuscating the truth about the source of an attack. *Id.*

determining the source of an attack is fraught with difficulties. For example, hackers can mask their location by writing the code at odd hours or in another language to avoid detection.[196] Thus, even the traditional tools of computer forensics—looking at the style used by the attackers, the timing, and the targets—only leave an idea as to who performed the attack.[197] The result, however, is still a guess, even if it is a very good guess.[198] This still does not conclusively prove any connection between the attackers and the Russian government.[199]

Furthermore, the differences between traditional weapon attacks and cyber-attacks are quite dramatic. While military tactics and intel can be shared without physical contact, sharing actual weapons requires delivery of tangible goods. As evidenced in the Georgia scenario, cyber weapons, particularly for more simple attacks such as denial of service attacks, can be "distributed" by merely posting information on an open website, then having would-be attackers read the website and perform the attack themselves, without the need for special equipment from any government actors.[200]

Quite simply, a government does not need to provide any physical equipment to private citizens to carry out the attack. Individuals can use their own computers or cell phones and Internet connections to launch attacks against locations throughout the world. Again, a simple posting on a website is all that is needed to provide "weapons," "training," and "guidance" regarding what private citizens need to do in order to carry out cyber-attacks. Contrast this with the training, arms, equipment, and information about troop movement that were given by the United States to the *contras* or the ninety percent of material support provided by Yugoslavia to the VRS.[201] Simple cyber-attacks require a much lower level of tangible and monetary support than physical altercations.

---

[196] *Id.*

[197] *Id.*

[198] A top-secret 2009 National Security Agency estimate rated Russia as the "most sophisticated adversary for the United States in cyberspace." Alpert, *supra* note 2. Thus, it seems reasonable to implicate Russia in the most advanced attacks that occur.

[199] *Id.* (noting that "researchers say hackers working for the Russian government" have been breaking into computer networks, including those of Georgia, for the past seven years, even though the report "does not cite any direct evidence" of involvement, based on the time the software was written, the Russian language settings of the computers, and that the targets align with Russian interests). The report went on to note, however, that distinguishing between attacks conducted by Russian cybercriminals and those purportedly conducted by the Russian government is often difficult. *Id.* One other key factor that "convinced . . . researchers that the campaign was the work of the Russian government" was the "professional, well-resourced effort" that went into the malware that took place over a seven-year period. *Id.* Similarly, a report on the "Sandworm" Campaign, a cyber espionage campaign targeting NATO, Ukraine, Poland, the EU, and energy companies, among others, was deemed as originating in Russia by iSIGHT Partners because it included a Russian directory listing, targeted institutions that would be of interest to Russia, was designed to appeal to personnel involved in operations against Russia, and the source code was released through Russian e-crime channels. *Russian Cyber Espionage Campaign* – Sandworm *Team*, ISIGHT PARTNERS (Oct. 14, 2014) 7, *available at* http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National-Security/Graphics/briefing2.pdf. One other factor that iSIGHT found in favor of attributing the campaign to Russia was the fact that the command server, which was located in Germany, was "inadvertently exposing Russian-language computer files that had been uploaded by the hackers." Ellen Nakashima, *Russian Hackers Use 'Zero-Day' to Hack NATO, Ukraine in Cyber-Spy Campaign*, WASH. POST (Oct. 13, 2014), http://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html.

[200] SHAKARIAN ET AL., *supra* note 65, at 25.

[201] *Supra* Part IV.A.

Even though average Russian citizens "could not have conduct[ed] [their] crucial or most significant" cyber-attacks without guidance (possibly from the Russian government through private websites), they would, similar to the scenario in *Bosnia & Herzegovina*, not be in a state of "total dependence" because they still maintained "some qualified, but real, margin of independence."[202] Ordinary Russian citizens, similar to the individuals described earlier, did not receive any call to action from the government—instead they were inspired by their own nationalistic feelings to launch attacks against Georgia.[203] It seems to stretch credulity to believe that loosely-associated individuals or even partially sponsored or allied youth groups such as Nashi would be considered in "complete dependence" on the Russian government despite any financial assistance they may receive from it.

Even the instructions, directions, or control standard of Article 8 is difficult to meet in this situation. Providing instructions on how to perform a denial of service attack or intimating that cyber-crime organizations would go unpunished if they stand ready to participate in activities that Russia requires both seem to indicate a degree of connection between the attackers and the government. But due to the limited evidence of communication between the two groups, it is difficult to say that Russia gave instructions or exercised control "in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken."[204] The very nature of cyber-crime in Russia is that of an unspoken agreement— groups are to take action in support of the government against outside forces and join in other efforts when they are taking place.[205] There is no need to wait for a request from the government. While directions were given in each case (instructions on how to perform a denial of service attack and sites to target), once again there is no connection between those instructions and the Russian government.[206] Instead, there appears to be a lack of any "effective control;" the Russian government allowed the citizens to act on their own, on behalf of their country. Even considering the potential funding of youth groups, the connection is too tenuous—*Nicaragua* involved significant and essential funding of paramilitary groups by the United States, but the groups' actions were still not attributable to the United States.[207]

The attacks against Target and other commercial retailers in the United States have an even more tenuous connection to the Russian government. Unlike Estonia and Georgia, and even the later attacks against Western financial institutions and energy companies, Russia does not seem to have any reason to target U.S. retailers. Of course, stealing funds from Western companies instead of Russian companies is definitely in line with the general agreement that seems to have been

[202] Application of Convention on Prevention and Punishment of Crime of Genocide (*Bosn. & Herz. v. Serb. & Montenegro*), 2007 I.C.J. 43 206 ¶ 394 (Feb. 26).

[203] Gvosdev, *supra* note 18, at 182.

[204] *Bosn. & Herz.*, 2007 I.C.J. 208 ¶ 400.

[205] *Supra* Part II.B.

[206] *See supra* Part III.A–B.

[207] Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.*), 1986 I.C.J. 61 ¶ 106 (June 17).

made between Russian hackers and the government, but there does not seem to be "complete dependence" or even instructions, direction, or control. Without any real connection to the Russian government, the attacks against Target and other U.S. businesses are even less likely to be attributable to Russia or to Russian hackers than are the other attacks mentioned above.

Going forward, it is likely that only attacks occurring at politically opportune times could ever be attributable to Russia under the framework established by *Nicaragua* and *Bosnia & Herzegovina*. Such an attack might be targeted against financial institutions in the aftermath of the introduction of financial sanctions against Russia or against energy companies after the introduction of sanctions prohibiting technological transfer from Western oil super majors to Russian companies. Because hackers have the ability to obfuscate information and misdirect any attempt to find the source of an attack and because outside countries are unable to see the communications between the Russian government and the attackers, the *Nicaragua* and *Bosnia & Herzegovina* framework does not provide much, if any, recourse for the victims of cyber-attacks.

B. Fittingness of Holding Russia Responsible Because of Its Hacker Culture

The somewhat older framework, as described in *Tellini*, *Corfu Channel Case*, and *Iran*, seem perfectly suited to meet the needs of protecting States. If a State is responsible for the actions of its citizens when it has "neglected to take all reasonable measures for the prevention of the crime and the pursuit, arrest[,] and bringing to justice of the criminal," then Russia's choice to not assist Estonia should implicate Russia as a responsible party.[208] While *Tellini* involved political crimes, its principle could be applicable here, particularly because Russia seems to allow citizens to use cyber tactics against foreign entities while vigorously preventing them from using the same tactics against its own government.[209] Furthermore, considering the rationale stated in *Iran*, even if a State is not involved in the initial actions of a rogue group of citizens, it is still under an obligation to take "appropriate steps" to prevent attacks or stop them—unless the State lacks the means to do so.[210] Again, Russia's prowess in cyber matters is not debatable—other than the United States, Russia is perhaps the most advanced cyber nation in the world.[211] It has "the means at [its] disposal" to, at the very least, slow down or stop attacks that are in progress (especially when the attacks continue for several weeks) and to search for those who are responsible and attempt to prosecute them. Thus, Russia's strong ability in this area, combined with its decision to not assist Estonia in stopping the attacks, finding the criminals, or even investigating the crimes, shows

[208] *See supra* Part III.A.
[209] *See supra* Part II.B.
[210] United States Diplomatic & Consular Staff in Tehran (*U.S. v. Iran*), 1980 I.C.J. 3, 31 ¶ 63 (May 24).
[211] *See* Gonsalves *supra* note 47; *see also* Pagliery *supra* note 195.

a significant degree of neglect, similar to what was described in both the *Tellini* and *Iran* cases.

Equally cogent is the argument made by the International Court of Justice in the *Corfu Channel Case*: "every State [has an] obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[212] By allowing groups of known hackers to continue unabated during times of peace and by not interfering to stop the hackers after cyber-attacks have begun, Russia is knowingly allowing "its territory to be used for acts contrary to the rights" of other nations—in this case Estonia. States have an obligation to stop their own citizens from harming other States, particularly after the victim State has reached out for assistance in dealing with the problem, as was the case with Estonia. This is due to the inherent disadvantages of not having physical access to the alleged perpetrators. States are much better positioned to control cyber-attacks that originate from within their borders, therefore States should have greater responsibility for controlling such actions.[213] For all these reasons, Russia should be held responsible for its inaction with respect to Estonia under the principles expressed in *Tellini*, *Corfu Channel Case*, and *Iran*.

This is not to say that any act by a private citizen should be answerable by the State. Some attacks are likely not preventable—they may happen without warning or are finished so quickly that *no* State could have responded to the action in time to prevent it. The Target incident, particularly as it relates to the purported author of the virus (but not necessarily as it regards those who actually used the virus), fits into this category. It is unlikely that a State will be able to prevent the creation of every virus that private citizens set out to create.[214] However, the latter portion of the *Tellini* principle—"tak[ing] all reasonable measures for . . . the pursuit, arrest[,] and bringing to justice"—are still implicated. Thus, the fact that a Russian minor quite possibly wrote the virus that was used against Target should not necessarily bring responsibility upon Russia. However, the fact that Russia did not pursue the individual or bring him to justice could be used to show that the country should be held responsible for his actions. Thus, Russia should be held responsible for the Target case as well.

Going forward, Russia should be subject to a higher level of responsibility than other States due to its history of allowing hackers to escape prosecution except when they target domestic institutions.[215] The highly provocative suggestion that Russia has handshake agreements with hacking groups only further implicates Russia as being complicit in the attacks that are happening and increases the ability to hold it responsible for not responding to attacks emanating from within its borders. While every State has a responsibility to respond to requests

[212] *Corfu Channel Case* (U.K. Gr. Brit. & N. Ir. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

[213] Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELB. J. INT'L L. 1, 2 (2013).

[214] It is also possible that the relatively open nature of the market for hacking tools and jobs in Russia would indicate that Russia *does* have the ability, to a certain extent, to seek out those who are offering their illegal services and stop them before they have a chance to sell their viruses. *See* Goncharov, *supra* note 44.

[215] *See supra* Part II.B.

from other States regarding potential attacks that are emanating from within their borders, Russia's history of malfeasance should increase the burden that Russia has in assisting the investigations of other nations regarding cyber-attacks perpetrated by Russian citizens.

Even without the strong hint of an outright agreement between hackers, criminal groups, and the Russian government, Russia's record of enforcement by itself seemingly implicates its responsibility. As discussed above, Russia has laws regulating intellectual property rights and cyber-crime, but it rarely enforces those laws and even more rarely doles out punishments that could possibly act as a deterrent given the lucrative rewards that flow to perpetrators of cyber activities.[216]

There are, however, some potential problems with placing such a burden on Russia. Even determining that an attack is originating from Russia is not clear-cut. The relatively simple nature of some cyber-attacks, such as denial of service attacks, makes it difficult, if not impossible, to conclusively find the source of the attack.[217] The attacks can originate from any location and the source addresses assigned to the attacks can be falsified.[218] Even if the message can be sourced correctly, the originating computer could be part of a botnet—the source computer might have been infected by a virus and might be controlled by another computer or individual in a different location.[219] As a result, it is possible for States to frame an innocent State for an attack that did not originate from within its borders.

Presumptively finding that Russia is the source of an attack could sour feelings between nations. Because of its past practices, it makes sense for hackers to mask their tracks through Russia to attempt to implicate Russia in future attacks. With the current degree of distrust between the West and Russia, a Western victim would likely take any opportunity to blame Russia for an attack. Again, however, it seems reasonable, given Russia's history of tacit (or active) support of hackers[220] and the greater physical access that Russia has to its own population, to require it to at least provide assistance to outside States when they have information implicating Russian citizens in the commission of attacks.

Another troubling implication of assigning State responsibility for the actions of private citizens is the possibility of greater governmental control over the Internet, particularly in those locations where there is already significant government control. Encouraging Russia to engage in a more severe form of access or content control, given its significant stake in a variety of Internet companies already,[221] may only serve to limit the ability of Russian citizens to access outside information. In addition, the significant disconnect between what Western nations want Russia to do and what Russian citizens expect—considering the current overall acceptance of hacking among the Russian population[222]—will

[216] *See supra* Part II.B.
[217] SHAKARIAN ET AL., *supra* note 65, at 15.
[218] *Id.*
[219] *Id.* at 15–16.
[220] *See supra* Part II.B.
[221] *See supra* Part II.B.
[222] *See supra* Part II.B.

make it difficult at best for the government to start to more strictly enforce laws against behavior that the population does not find morally wrong.

While there is not much recent precedent regarding holding a State responsible for not adequately preventing or responding to attacks of private individuals or groups, Russia seems like an ideal place to hold the State accountable. The fact that violations of intellectual property rights and cyber-crime often go unpunished implicates Russia as not having taken "reasonable measures" to prevent and prosecute the perpetrators of such acts, especially given its extraordinary strength in this area.

VI. CONCLUSION

There is a significant incentive for countries to allow hacker groups within their borders to attack foreign countries. As long as States are not held responsible for the actions of independent groups within their borders, they will not feel the need to control or mitigate the effects of these groups on outside nations. Furthermore, the relative imbalance of power between the attackers and the victims is evident. Targets can be chosen precisely, as evidenced in the Estonia and Georgia cases. Attributing the effects of those attacks cannot be done with anything even closely approximating the precision of the attacks. This asymmetry currently encourages States to do little to stop cyber acts emanating from within their borders because the negative effects are felt outside of the borders. On the other hand, preventing or mitigating the attacks would internalize the costs without necessarily providing any additional benefit.

The current attribution rules as found in the *Responsibility of States for Internationally Wrongful Acts* are inadequate to enforce and maintain peace in an increasingly cyber-dominated world. A resurgence of the responsibility models of earlier case decisions will help States to be protected and have recourse for cyber attacks against them. This will be possible due to the capabilities of States to regulate the conduct of private citizens and groups within their borders.

Based on Russia's lax enforcement mechanisms of cyber-crime—intellectual property related and in other areas—Russia should be held to a higher standard than other States. It is one thing for a rogue individual to attack an outside State. It is quite another for a State to ignore the actions of its citizens and to choose not to pursue them when it is aware of the damages that the citizens are causing outside of its borders. Russia should be held responsible for the actions of its citizens, especially when those actions are of a long duration or when Russia fails to stop the attacks or to prosecute those who engaged in them.