BYU Law Review

Volume 2015 | Issue 1 Article 7

February 2015

Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-boundary Cybercrime

Daniel Ortner

Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-boundary Cybercrime

I. INTRODUCTION

In December 2013, 110 million consumer accounts were hacked as a result of a security breach at Target—probably the largest security breach in U.S. history.[1] It was subsequently disclosed that the hackers used Russian-made malware to pull off the attack. Although unconfirmed, many analysts suggested that the Russian Mafia orchestrated the breach.[2]

In Russia, an extremely profitable and professional cybercrime industry[3] has emerged. Overall, Russian hackers have been responsible for a disproportionate share of cybercrime.[4] In 2013, the Russian cybercrime industry made at least $1.9 billion dollars.[5] Russian-speaking countries also contribute significantly to overall cybercrime.[6] Much of the crime is attributable to organized groups, such as the Russian Mafia.[7]

1. Kacper Pempel, *Largest Single Personal Data Hack Ever? 360mn Stolen Account Credentials Found Online*, RT (Mar. 1, 2014 1:31 AM), http://rt.com/news/largest-hack-stolen-credentials-287/.

2. *See* Walter Russell Mead, *Russian Mob May be Behind Target Hacking*, THE AMERICAN INTEREST (Jan. 17, 2014 12:20 PM), http://www.the-american-interest.com/blog/2014/01/17/russian-mob-may-be-behind-target-hacking/.

3. The department of Justice classifies cybercrimes into three categories: (1) Cyber attacks – crime where the computer system is the target, such as viruses, DoS attacks and other sabotage or vandalism; (2) Cyber theft – where a computer is used to steal money through extortion, embezzlement or other means; (3) Other Computer Security Incidents: breaches such as phishing, adware, or theft of information. *See* U.S. DEPT. OF JUSTICE, CYBERCRIME AGAINST BUSINESS, 2005, BUREAU OF JUSTICE STATISTICS, *available at* http://www.bjs.gov/content/pub/pdf/cb05.pdf. This Comment is primarily concerned with either cyber attacks or cyber theft as such crimes tend to have significant or substantial consequences sufficient to trigger the international due diligence obligation.

4. *Global Security Report May 2012*, GROUP IB, http://www.group-ib.com/images/media/global_security_report_201205.pdf.

5. John Casaretto, *Report: Russia's CyberCrime Market Hits $1.9 Billion*, SILICONE ANGLE (Oct. 9, 2013), http://siliconangle.com/blog/2013/10/09/report-russias-cybercrime-market-hits-1-9-billion/.

6. Jarrod Rifkind, *Cybercrime in Russia*, CENTER FOR STRATEGIC & INT'L STUD. (Jul. 14, 2011), https://csis.org/blog/cybercrime-russia.

7. I will use the phrase Russian Mafia interchangeably with Russian organized crime. For an

The cost of cybercrime is even greater than those statistics suggest. One study, which included the costs of clean up after an attack but not the additional costs of lawsuits filed after a breach, concluded that cybercrime cost $113 billion dollars.[8]

The increased prevalence of trans-boundary cybercrime, coupled with Russia's unwillingness to aggressively pursue the Russian Mafia and other cybercriminals, leads to the question of whether Russia has an international obligation to prevent such crimes. So far, Russia has refused to sign on to the Council of Europe Convention on Cyber Crime, in part due to its reluctance to take upon itself an obligation to cooperate in the investigation of the numerous cyber-attacks caused by its residents or using its infrastructure.[9] Likewise, because of the difficulty of establishing direct attribution or complicity, Russia has thus far not been held accountable for failure to prevent cyber-attacks such as those that were launched against Estonia in 2007 and 2008 or the ongoing cybercrime carried out by Russian organized crime.[10]

This Comment argues that *Russia has an obligation to monitor and prevent trans-boundary cybercrime under the standard of due diligence*. Due diligence has never been applied directly to cybercrime, but it is increasingly viewed as a general obligation and customary expected state conduct.[11] It is a concept deeply rooted in international law in a wide variety of fields including environmental law, human rights, and the prevention of crime. Moreover, Russia's involvement in such treaties as the Convention against Transnational Organized Crime [Palermo Convention] implies that Russia has accepted at least parts of this duty of due diligence.[12]

overview of the structure of the Russian Mafia, see JAMES O. FINCKENAUR & YURI A. VORONIN, THE THREAT OF RUSSIAN ORGANIZED CRIME, U.S. DEPARTMENT OF JUSTICE (2001).

8. Willie Jones, *How Much Does Cybercrime Cost? $113 Billion*, IEEE SPECTRUM (Nov. 22, 2013 23:12 GMT), http://spectrum.ieee.org/riskfactor/telecom/security/how-much-does-cybercrime-cost.

9. *Putin Defies Convention on Cybercrime*, C NEWS (Mar. 27, 2008 10:04:15), http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913.

10. Casimir C. Carey III, *The International Community Must Hold Russia Accountable for its Cyber Militias*, SMALL WARS J. (Mar. 27, 2013 2:30 AM), http://smallwarsjournal.com/jrnl/art/the-international-community-must-hold-russia-accountable-for-its-cyber-militias.

11. *See infra* Part III.

12. *See infra* Part IV.

Part II of this Comment will look at the inadequacy of alternative grounds for holding Russia responsible such as direct attribution or complicity. In Part III, the standard of due diligence will be discussed in depth. Particular attention will be given to the question of what standard of due diligence should be enforced in the cyber context. Russia's additional treaty obligations under the Palermo Convention also supplement its obligation under customary law and will be considered in Part IV. Having established a possible standard for due diligence, Part V. will then describe the Russian Mafia and Russia's efforts to prevent organized cybercrime. In Part VI., Russia's efforts will be held up to the standard of due diligence to show that Russia has fallen short of its due diligence obligation to prevent trans-boundary cyber-attacks and cybercrime from its territory. Finally, in Part VII, this Comment will conclude on a hopeful note by looking at a new Russian proposal that if passed and fully implemented would likely meet the State's due diligence obligation.[13]

II. DIFFICULTY OF PROVING DIRECT ATTRIBUTION OR COMPLICITY FOR CYBERCRIME AND CYBER-ATTACKS

One possible way that Russia could be held accountable for its failure to prevent trans-boundary cybercrime is through its direct involvement in the attacks, or through knowing complicity.[14] In particular, Russia was accused of either being directly responsible for—or at the very least complicit—in the wide-ranging cyber-attacks that crippled neighboring Estonia in 2007 and 2008.[15] For instance, tools used by hackers were stored on government servers and infrastructure and attacks came from government IP addresses.[16] Scholars have written about the Estonia conflict and debated

14. For an explanation of complicity and its relationship to state responsibility, see generally, HELMUT PHILIPP AUST, COMPLICITY AND THE LAW OF STATE RESPONSIBILITY (2011). *See also* Vassilis P. Tzevelekos, *In Search of Alternative Solutions: Can the State of Origin Be Held Internationally Responsible for Investors' Human Rights Abuses That Are Not Attributable to It?*, 35 BROOK. J. INT'L L. 155, 170–75 (2010).

15. *See Behind the Estonia Cyberattacks*, RADIO FREE EUROPE (Mar. 6, 2009), http://www.rferl.org/content/Behind_The_Estonia_Cyber-attacks/1505613.html [hereinafter *Behind the Estonia Cyberattacks*]; *see also* Carey, *supra* note 10.

16. *Behind the Estonia Cyberattacks*, *supra* note 15; *See also* Arthur Bright, *Estonia Accuses Russia of 'Cyberattack,'* CHRISTIAN SCIENCE MONITOR (May 17, 2007), http://www.csmonitor.com/2007/0517/p99s01-duts.html.

whether Russia was directly responsible or complicit in the attacks due to the highly sophisticated and coordinated nature of the attacks.[17] However, the government has strongly denied any complicity or direct involvement.[18] In the recent conflict with Ukraine over the Crimea, cyber-attacks and disruptions of services also coincided with the deployment of troops.[19]

Yet, despite some limited evidence of direct involvement or complicity, Russia is unlikely to be held responsible for direct involvement or complicity. The standard set out by the International Court of Justice (ICJ) for such a charge is quite difficult to prove. In the *Corfu Channel Case*, the seminal case on attribution, the ICJ rejected a British argument that Albania was responsible through "acquiescence" and "collusion" for mines that led to the destruction of British ships.[20] In rejecting this argument, the ICJ suggested that such a charge of "exceptional gravity" required a "degree of certainty" that the British had been unable to prove.[21]

While some cyber-attacks have been successfully decoded and tentatively attributed to their sources,[22] such attribution is unlikely in the wide range of cyber-attacks being carried out from Russia on an ongoing basis.[23] Determining origin is a time intensive and inconclusive endeavor as shown by the efforts to decode Stuxnet—the cyber weapon that was used to sabotage Iran's nuclear

17. *See* Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 J. STRATEGIC SECURITY, Summer 2011, 49 (2011).

18. *See* Nate Anderson, *Massive DDoS Attacks Target Estonia; Russia Accused*, ARS TECHNICA (May 14, 2007 6:45 AM), http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/. A member of the Russian Duma allegedly has stated that one of his aides was responsible for the attack, but the official Russian position has been to deny any involvement. *See Behind the Estonia Cyberattacks*, *supra* note 15.

19. *Ukraine Crisis: Ukraine's Telecommunications Hit by Cyberattacks*, REUTERS (Mar. 4, 2014), http://www.straitstimes.com/breaking-news/world/story/ukraine-crisis-ukraines-telecommunications-hit-cyber-attacks-20140304. *But see* Mark Clayton, *Where are the Cyberattacks? Russia's Curious Forbearance in Ukraine*, CHRISTIAN SCIENCE MONITOR (Mar. 3, 2014), http://www.csmonitor.com/World/Security-Watch/2014/0303/Where-are-the-cyber-attacks-Russia-s-curious-forbearance-in-Ukraine.-video.

20. *See* Corfu Channel Case (U.K. v. Alb.) 1949 I.C.J. 4 (Apr. 9).

21. *Id.* at 17.

22. *See* Ellen Nakashima & Joby Warrick, *Stuxnet was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 2, 2012), http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

23. Because attacks can originate from machines around the world, pinpointing the controller or designer of a specific attack is highly imprecise. *See* Anderson, *supra* note 18.

program.[24] Moreover, any government complicity with the Russian Mafia's cyber activities is most likely attributable to corruption or bribed officials rather than official government policy.[25] Thus, evidence of complicity is likely to be sparse and insufficient. It is unlikely that such a "degree of certainty" will ever be established regarding cybercrimes.[26]

In addition, even if sufficient evidence existed, liability through complicity and direct attribution is generally limited in scope because it would only apply to those cases where complicity or direct attribution could be proved.[27] In other words, even if the Russian government's responsibility for the attacks in Estonia were firmly established, it would do little to establish a more general state responsibility for the trans-boundary harm caused by non-state actors. Therefore, despite some evidence of complicity between the Mafia and the Russian government, complicity or direct attribution are unlikely to provide adequate grounds for state liability. This Comment seeks to establish an alternative and more general basis for Russian responsibility for trans-boundary cybercrime based on the principle of due diligence

III. DUE DILIGENCE STANDARD IN INTERNATIONAL LAW

While international law does not impose strict responsibility upon a state for injuries suffered by a foreign state as a result of its conduct or the conduct of its citizens, states are generally seen as responsible for negligent conduct.[28] More specifically, a state is

24. *Id*. For an in depth look at the painstaking efforts required to decode Stuxnet, see Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July, 11, 2011), http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/1.

25. For a description of Mafia influence and corruption in the judicial system, see *infra* Part VI. For an overview of attribution of conduct to a state generally, see U.N. LEGISLATIVE SERIES, MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, 27–96 (2012), *available at* http://legal.un.org/legislativeseries/documents/Book25/Book25_part1_ch2.pdf.

26. For a detailed analysis of various proposed standards of proof for state responsibility, see Scott J. Shackelford and Richard B. Andres, *State Responsibility for Cyber-attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971 (2011).

27. *See* MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, *supra* note 25.

28. OPPENHEIM'S INTERNATIONAL LAW, Vol. 1, 508–11 (Sir Robert Jennings QC & Sir Arthur Watts KCMG QC eds., 9th ed. 2008).

required to exercise due diligence to prevent citizens or others residing within its territory from committing trans-boundary harm.[29]

It is well established in international law that states are required to prevent the use of their territory or resources to cause injury to another state or citizens of another state.[30] For instance, in the *Trail Smelter Arbitration*, the United States was damaged by fumes and industrial pollution emanating from Canadian businesses across the border.[31] The tribunal concluded that Canada was responsible for the harm caused by the Trail Smelter because "no State has the right to use or permit the use of its territory in such a manner as to cause injury . . . in or to the territory of another or the properties or persons therein . . . ."[32] The *Trail Smelter Case* is considered one of the primary sources of the enduring doctrine of due diligence.[33]

Due diligence is the most commonly applied standard for the state's duty to prevent trans-boundary harm.[34] It is a robust standard with widespread application in various fields of international law. The next section describes the history and the wide acceptance of the standard of due diligence. The specific contours of due diligence as applied to cybercrime will then be developed and elaborated upon.

A. Due diligence is a well-established principle with a strong historical pedigree

The standard of due diligence has a lengthy historical pedigree.[35] Due diligence is based on the historic maxim of *sic utere*

29. *Id*. at 549.

30. *Id*.

31. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905 (Trail Smelter Arb. Trib. 1941), http://legal.un.org/riaa/cases/vol_III/1905-1982.pdf.

32. *Id*. at 1965.

33. Mark A. Drumbl, *Trail Smelter and the International Law Commission's Work on State Responsibility for Internationally Wrongful Acts and State Liability*, TRANSBOUNDARY HARM IN INTERNATIONAL LAW, (Russell A. Miller ed., 2006) *available at* http://law.wlu.edu/faculty/links/chapter8drumbl.pdf.

34. Nevertheless, despite its important role, some have argued that due diligence as a standard has received inadequate scholarly coverage. *See*, *e.g.*, Gabe Shawn Varges, *Book Review*, 85 AM. J. INT'L L. 568 (1991) (reviewing RICARDO PISILLO MAZZESCHI, 'DUE DILIGENCE' E RESPONSABILITÀ INTERNAZIONALE DEGLI STATI (Dott. A. Giuffrè ed., 1989)). This Comment is an attempt to add to that discourse.

35. One sign of the widespread permanence of the concept of due diligence is that the English term is commonly used even when the concept is discussed in countries with languages that have equivalent or analogous terms in the native tongue. *See* Varges, *supra* note 34 (for instance, *diligence requise* in French and *diligenza dovuta* in Italian).

tuo ut alienum non laedas and has its origin in Roman law.[36] Due diligence was a central concern in early efforts to codify rules of state responsibility.[37] Even though codification efforts have failed, there is a general consensus that the obligation of due diligence is part of the "corpus of general international law."[38] Despite the lack of general codification, due diligence has been applied in many fields, ranging from international environmental law,[39] and efforts to prevent violence against women,[40] but it applies to all areas of international law.[41]

Likewise, due diligence has played a prominent role in important international law decisions. An arbitration in 1902 over economic losses suffered by an Italian citizen in Venezuela held that "if . . . it is . . . proved that Venezuelan authorities failed to exercise *due diligence* to prevent damages from being inflicted by revolutionists, that country should be held responsible.[42] In 1924, after the assassination of an Italian general and other officials in Greece (Janina-Corfu affair), a Commission of Jurists appointed by the League of Nations explained that a state is responsible for harm committed against foreigners "if the state has neglected to take all reasonable measures for the prevention of the crime."[43] The Commission also recognized a concomitant obligation to pursue perpetrators and ensure that they are brought to justice.

36. So use your own as not to injure another's property. *See* Jutta Brunnée, *Sic utere tuo ut alienum non laedas*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (2010).

37. Timo Koivurova, *Due Diligence*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (2010).

38. *Id*.

39. A wide range of environmental treaties incorporate the standard of due diligence. *See* PATRICIA BIRNIE, ALAN BOYLE & CATHERINE REDGWELL, INTERNATIONAL LAW & THE ENVIRONMENT 147–50 (2009).

40. Special Rapporteur on Violence against Women, its Causes and Consequences, *Report of the Special Rapporteur on violence against women, its causes and consequences*, COMM'N ON HUMAN RIGHTS, U.N. Doc. A/HRC/23/49 (May 14, 2013) (by Rashida Manjoo), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A_HRC_23_49_English.pdf.

41. Koivurova, *supra* note 37 ("[I]n international law the concept of due diligence remains a general principle of law.").

42. Salvatore Sambiaggio (It. v. Venez.), 10 R.I.A.A. 499 (Mixed Claims Comm'n, 1902) (emphasis added).

43. David Jayne Hill, *The Janina-Corfu Affair*, 18 AM. J. INT'L L. 98 (1924). *See also* Quincy Wright, *Opinion of Commission of Jurists on Janina-Corfu Affair*, 18 AM. J. INT'L L. 536 (1924).

Other international courts have also invoked the standard of due diligence. For instance, the ICJ determined in 1979 that the government of Iran had failed to take "appropriate steps" to protect the United States consulate, and that its failure "was due to more than mere negligence or lack of appropriate means."[44] While the ICJ did not explicitly mention due diligence, the concept is implicit in language referring to "appropriate steps."[45] Likewise, in *Nicaragua v. United States*, the ICJ held that Nicaragua would not be held to a "higher degree of diligence" to control arms traffic than wealthier nations such as the United States.[46] Implicit in the court's analysis is that states do owe some degree of diligence in responding to and preventing trans-boundary harm.

Thus, the existence of a due diligence obligation to prevent trans-boundary harm is well attested in customary international law and international legal precedent. The next section will flesh out the contours of a state's due diligence obligation.

B. What duty of care is required under due diligence?

One of the challenges in regard to due diligence is determining exactly what standard of duty of care is required of states. Compounding this difficultly is the existence of slightly different conceptions of due diligence in different fields of international law. For instance, many of the specific contours of due diligence have developed in specialized fields such as international environmental law[47] and human rights law[48] (especially in the effort to prevent violence against women), and may not always be generally applicable or widely accepted. Nevertheless, the many references to due

44. U.S. Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 63 (May 24).

45. Due diligence is implicit because appropriate steps implies that there is some minimal degree of conduct required of states. Some have suggested that the absence of the phrase "due diligence" can be attributed to fact that due diligence serves as a "generic notion" of responsibility which finds varied expression in different fields of international law. Tzevelekos, *supra* note 14. While this Comment attempts to argue that a general standard of due diligence can be synthesized, this may be why the exact phrase "due diligence" is absent even when implied.

46. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27) [hereinafter the *Nicaragua case*]. The *Nicaragua case* will also be discussed later in the context of factors that impact the degree of diligence demanded of a state. *See infra* text accompanying notes 68–69. *See also* Koivurova, *supra* note 37.

47. *See* BIRNIE ET AL., *supra* note 39.

48. *See infra* notes 82–88 and accompanying text.

diligence in these disparate fields suggest a general standard that can be applied in the trans-boundary cybercrime context.[49] This section will explore the standard of due diligence and attempt to synthesize the various obligations.

In subsection 1, I will consider what kinds of trans-boundary harm trigger a state's due diligence obligation. Next, subsection 2 will discuss the degree of care required under the standard of due diligence. Subsection 3 will look into the specific state obligations, specifically the duties to prevent, protect, prosecute, and redress.[50] Throughout, specific applicability of these standards in the cybercrime context will also be considered.

1. Triggers for trans-boundary harm

According to the United Nations' International Law Commission (ILC), harmful conduct qualifies as trans-boundary harm when four criteria are met: First, the activity in question must be human activity. Second, it must be within the territory or control of one state. Third, it must give rise to harm or be capable of giving rise to harm. Fourth, that harm must be to persons or things within another state.[51]

For cybercrime, human activity should be viewed quite broadly. A broad view of human activity is necessary because of the potential for self-replicating or spreading viruses or bots.[52] If continuous human control were required before due diligence applied, state responsibility would be drastically limited. It would also provide an exploitable loophole for a state hoping to escape liability. Instead, cybercrime should qualify as human activity if the programming or activity has a human origin. This broad definition of human activity

49. Even though a general standard can be synthesized from disparate cases and references to due diligence, drafting and ratifying a comprehensive convention on cybercrime would be helpful in solidifying the exact obligations of a state. Thus, the existence of a general standard should encourage efforts to create specific international agreements and norms. *See* Tzevelekos, *supra* note 14.

50. Special Rapporteur on Violence against Women, its Causes and Consequences, *The Due Diligence Standard as a Tool for the Elimination of Violence against Women*, Comm'n on Human Rights, U.N. Doc. E/CN.4/2006/61 (Jan. 20, 2006) (by Yakin Ertürk).

51. Daniel Barstow Magraw, *Transboundary Harm: The International Law Commission's Study of "International Liability"*, 80 AM. J. INT'L L., 305, 310 (1986).

52. Stuxnet was a self-replicating virus for instance, and spread far beyond the originally intended target. *See* Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, 63 JOINT FORCE QUARTERLY 70 (2011).

is consistent with the ILC's wording, which was mainly understood to exclude natural disasters and other acts of nature.[53]

In regard to cybercrime, one of the more difficult questions is whether a cybercrime occurs under the control of a state. For instance, if a cybercrime originates in territories that are indirectly controlled by Russia such as Chechnya or Crimea, it is not certain what degree of control the state has. However, the obligation of due diligence is incumbent upon each nation regardless of whether that nation has sufficient control to fully prevent the cybercrimes from occurring.[54] A state is responsible for doing what is actually within its power; for instance, the European Court of Human Rights (ECtHR) found Moldova and Russia responsible for its failure to exercise due diligence "even in the absence of effective control" to prevent an arbitrary detention. [55] Under the European Convention, Moldova and Russia had the responsibility to "take the diplomatic, economic, judicial or other measures that it is in its power to take . . . ."[56] Thus, the international and diffused nature of cyber activities does not justify laxity on the part of states. While it may be difficult to determine the point of origin of an attack, a state is still responsible for making efforts to prevent trans-boundary harm caused by those residing in its territory or through its cyber infrastructure.

The ILC's third criterion is that the conduct must give rise to harm or be capable of giving rise to harm. The requirement "that harm must be to persons or things within another state" is an expansive one. Because harm can be to things, that would include servers, files, or other hardware damages as a result of a cyber attack. However, one possible limitation on the scope of what qualifies as trans-boundary harm might be a requirement that the harm result in physical consequences.[57] For instance, under the Draft Articles on Prevention of Trans-boundary Harm from Hazardous Activities, conduct for which states are responsible extends to "any activity which involves the risk of causing significant transboundary harm through

53. *Id*.

54. *See* Tzevelekos, *supra* note 14, at 225.

55. Ilaşcu v. Moldova, 2004 Eur. Ct. H.R., 318 at ¶ 331.

56. While *Ilaşcu* focused on human rights violations under the European Convention, there is nothing in the decision that implies that the principle be limited only to violations of human rights.

57. *See* Magraw, *supra* note 51.

the physical consequences."[58] However, as the main focus of the Draft Articles is environmental harm, such a restriction may not be appropriate in the cyber context. Nevertheless, even with such a restriction, a great portion of cybercrime would qualify. It is arguable that altering code or causing a site to crash as a result of a DDoS attack[59] has physical consequences.[60] And certainly, a cybercrime that cripples critical governmental or civilian infrastructure would have dramatic physical consequences that extend beyond the realm of economic impact. Additionally, the harm need not be exclusively trans-boundary or exclusively impact those in another state.[61] Given the interconnected nature of the cyber economy, a cyber-attack might have consequences in both the country of origin and the target country. Such attacks would qualify as causing trans-boundary harm.[62]

In addition to the aforementioned requirements, in order for a state to be responsible for third party trans-boundary harm, the harm caused must be more than de minimus; the harm must be "significant."[63] Significant harm would include harm that is more than merely "detectible" and could be measured by objective standards including economic loss.[64] However, for harm to qualify as significant it need not rise to the level of serious or substantial.[65] Unfortunately, this distinction has not always been applied consistently. For instance, the *Trail Smelter Arbitration* relied on existing U.S. and international decisions to establish that the harm must be of serious consequence

58. Rep. of the Int'l Law Comm'n, U.N. GAOR, 53d Sess., U.N. Doc. A/56/10 (Apr. 23–June 1, July 2–Aug. 10, 2001); U.N. GAOR, 56th Sess., Supp. No. 10 (2008), http://legal.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf.

59. DDoS attacks typically occur when an attack floods a network or website with information causing an overload that leads to slowdown or a crash. *See US-CERT, Security Tip (ST04–015): Understanding Denial-of-Service Attacks* (Feb. 06, 2013), https://www.us-cert.gov/ncas/tips/ST04-015.

60. *See* Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, 2012 4TH INT'L CONF. ON CYBER CONFLICT (2012), *available at* http://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf (arguing that currently manipulation of data does not count as physical consequences to qualify as an armed attack, but that the proliferation of cyber-attacks might lead the standard to change).

61. *See* Magraw, *supra* note 51.

62. *Id.*

63. *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, A/56/10 International Law Commission (2001), art. 2 commentary (4).

64. *Id.*

65. *Id.*

and be established by clear and convincing evidence.[66] Nevertheless, cyber-attacks will regularly rise to the level of significant and, because of the staggering economic costs totaling in the millions or billons, may rise even to the level of having serious consequences. Certainly, the economic cost of Russian cyber-attacks on the U.S. rises to the level of having serious consequences.

2. Reasonableness

Due diligence is a standard of reasonableness, and therefore is assessed based on the standard of conduct expected of a reasonable government.[67] Due diligence is an "obligation of conduct rather than of result."[68] Thus, in assessing whether a state exercised due diligence, the focus is on what the state did or did not do to prevent cybercrime rather than whether its attempts succeeded.[69]

A range of factors, such as the degree of effective territorial control, resources available to a state, and the nature of specific activities are considered when determining what degree of diligence is required by a state.[70] In addition, the degree of risk is a vital consideration, with ultra-hazardous activities requiring a far higher standard of care and greater state diligence.[71] One historic example of the interplay of some of these factors is the ICJ's decision in the

66. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (Trail Smelter Arb. Trib. 1941), http://legal.un.org/riaa/cases/vol_III/1905-1982.pdf.

67. *See* Koivurova, *supra* note 37, at ¶ 16.

68. David Freestone, *Advisory Opinion of the Seabed Disputes Chamber of the International Tribunal for the Law of the Sea on 'Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, 15 AMER. SOC. INT. L. (March 2011), *available at* http://www.asil.org/insights/volume/15/issue/7/advisory-opinion-seabed-disputes-chamber-international-tribunal-law-sea-#_ednref10.

69. By a focus on efforts rather than results, I mean that a state will be judged based on whether adequate measures are in place to prevent a type of trans-boundary harm, rather than on whether those efforts were successful in preventing a particular harm. Thus, if a state has in place adequate measures to guard against trans-boundary cybercrime, it will not be responsible if a particular attack occurs despite its diligent efforts to prevent it.

70. The ICJ considered these factors in its decision in the *Nicaragua case* when it considered that the United States with its wealth had been unable to stem the flow of arms, and so it was unreasonable to expect far-less-prosperous Nicaragua to do so. *See also supra* note 69 and accompanying text.

71. Report of the International Law Commission to the General Assembly, *Prevention of Transboundary Harm from Hazardous Activities*, U.N. GAOR 53d Sess., Supp. No. 10, U.N. Doc. A/56/10, at 394 (2001), *reprinted in* [2001] 2 Y.B. INT'L L. COMM'N 148, 154, U. N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) (art. 3 cmt. 11), *available at* http://www.un.org/documents/ga/docs/56/a5610.pdf.

Nicaragua case. In that case, the ICJ applied and weighed the above factors against the risk created by the arms-traffic problem, and determined that the poorer state of Nicaragua could not be held responsible for failing to control the arms-traffic problem that its far-wealthier neighbors in the north could not even control despite superior resources.[72] The court also noted that Nicaragua had limited control of the flow of arms by "traditional smugglers" in Nicaraguan coastal areas and therefore could not expected to prevent all smuggling.[73]

Several other mitigating factors might also limit the degree of diligence a state is required to exercise. For instance, in the context of efforts to prevent violence against women, the ECtHR, has acknowledged some additional factors that play into assessing whether a state exercised reasonable due diligence. The ECtHR has suggested that a state's due-diligence obligation may be constrained by factors such as the "unpredictability of human conduct and operational choices which must be made terms of priorities and resources."[74] The ECtHR has also acknowledged a great degree of state discretion within the "margin of appreciation"[75] regarding appropriate legislative and judicial solutions.[76] Some have suggested that this test closely resembles the test of proportionality often used by the ECtHR in other contexts.[77] Thus, an inquiry into due

72. *See* Nicar. v. U.S., 1986 I.C.J. 14, ¶ 154 (June 27); *see also* Koivurova *supra* note 37, at ¶ 40.

73. *Id*. at ¶ 155.

74. Makaratzis v. Greece, App. No. 50385/99, 2004 Eur. Ct. H.R.; *See also* Lee Hasselbacher, *State Obligations Regarding Domestic Violence: The European Court of Human Rights, Due Diligence, and International Legal Minimums of Protection*, 8 NW. J. INT'L HUM. RTS. 190, at ¶ 39–40 (2010).

75. The notion of a margin of appreciation in the cyber context is worthy of further exploration. Taken to an extreme, it is a concept that can easily be abused. Certainly, the concept of a margin of appreciation cannot justify using the excuse of combating cybercrime as a pretext for censorship or aggressive violations of human rights, such as freedom of expression or freedom of religion. Nevertheless, when assessing whether a state's attempts to stop cybercrime are reasonable, unique national factors should be considered and weighed.

76. *See* Hasselbacher, *supra* note 74, at ¶ 36.

77. *See* Tzevelekos, *supra* note 14, at 203–04. Tzevelekns discusses the relationship between the margin of appreciation and the proportionality test in his article. He states that after the " court reaches regarding the extent of positive state obligations will undergo one last test, carried out at the macro, or generic, level of the due diligence principle. The baseline for this test is that the state has at its disposal the necessary means for providing the measures that have been considered reasonable in a given case." *Id*. at 204. He suggests that the margin of discretion that comes in depends upon the means of the state and other factors. *Id*.

diligence take into account other challenges a state faces as well as unique efforts that the state adopts to combat trans-boundary harm.

To determine whether a state has acted with due diligence in the context of cybercrime, one should consider the degree of technological development in a country (as a measure of wealth), and the degree to which the state has control over cyber infrastructure. The seriousness of potential cyber-attacks would also determine the expected degree of diligence. Accordingly, a state might be expected to spend much more energy combating cyber terrorism or large-scale organized activity than sporadic and less-dangerous activities perpetuated by isolated individuals.

Because due diligence relies on a standard of reasonableness, it has been criticized for providing little guidance on what specific legislation or actions a state must take;[78] nevertheless, the standard provides a degree of flexibility that is necessary as states attempt to combat intricate and complex modern problems. Importantly, the existence of the standard of due diligence implies that there is a level of minimally expected diligence by a state.[79] Moreover, a concurrent implication is that the standard is an evolving one requiring continuing improvements on the part of states. Indeed, due diligence has been described as a variable concept that changes over time and increasingly demands more of states in light of new scientific or technological knowledge.[80]

As states continue to develop technological capabilities, the standard of diligence for protecting and preventing cyber-attacks and cybercrime should continue to increase.[81] New scientific or technological knowledge regarding cyber-weapons should lead to increased capacity to prevent trans-boundary cybercrime. Over time,

78. BIRNIE ET AL., *supra* note 39. Indeed, due diligence has been accused of being simply a tautology and not a standard. Yet because the standard is an objective one based on the conduct of nations, generally, it can best be seen as an effort to "objectivize" fault rather than merely stating wishful thinking. *See* Gabe Shawn Varges, '*Due Diligence' e Responsabilita Internazionale Degli Stati by Riccardo Pisillo Mazzeschi*, 85 AM. J. INT'L L. 568 (1991) (attempts to give some "teeth" to the standard of due diligence).

79. Tzevelekos, *supra* note 14.

80. DONALD K. ANTON ET AL., ADVISORY OPINION ON RESPONSIBILITY AND LIABILITY FOR INTERNATIONAL SEABED MINING (ITLOS CASE NO. 17): INTERNATIONAL ENVIRONMENTAL LAW IN THE SEABED DISPUTES CHAMBER (2011), *available at* https://www.academia.edu/669708/Advisory_Opinion_on_Responsibility_and_Liability_for_International_Seabed_Mining_ITLOS_Case_No._17_International_Environmental_Law_in_the_Seabed_Disputes_Chamber.

81. *Id.*

the standard of care expected of states should increase rather than decrease as cyber-threats become more sophisticated and dangerous. As will be discussed further, states have an obligation to continually improve technological capabilities to respond to cybercrime.[82]

3. Specific requirements of conduct

Although states have an obligation to monitor and prevent trans-boundary harm, many have persuasively argued that there is a broader obligation to "prevent, protect, prosecute, and redress" cybercrime.[83] Merely monitoring and preventing is insufficient absent adequate police action and adequate prosecution to deter subsequent crime.[84] Likewise, without redress, such as access to civil courts or other remedial schemes, states fail to remedy the consequences of trans-boundary harm.[85] For a state to adequately and diligently respond to trans-boundary harm caused by its citizens, each of these components should be required.[86]

Thus, due diligence can be seen as an affirmative obligation requiring a state to do more than merely respond to harm already caused. States must take "preventive measures" or, at the very least, minimize the impact of trans-boundary harm.[87] Where states are unable to fully prevent harm, there is still a duty to minimize the risk of such harm.

Before delving into the specific requirements of state conduct under due diligence, it is helpful to look at an example of how this

82. *See infra* text accompanying note 96.

83. Special Rapporteur on the Violence Against Women, its Causes and Consequences, *Integration of the Human Rights of Women and the Gender Perspective: Violence Against Women*, ¶ 29, Comm'n on Hum. Rts., U.N. Doc. E/CN.4/2006/61 (Jan. 20, 2006) (by Yakin Ertürk). The ILC proposed a slightly different but similar framework of four "compound obligations" to prevent, inform, negotiate, and repair. Given that the ILC was focused on harmful acts that are not illegal, the absence of a prosecutorial component is expected. Still, the similarities suggest a general agreement that something more than mere prevention is required. *See* Magraw, *supra* note 51, at 311.

84. *See infra* Part III.B.3.a–c.

85. See *infra* Part III.B.3.d.

86. Of course, there is considerable overlap between concepts such as prevention and protection. Classification of one approach as either preventive or protective is made on the judgment of the author. As the concept of due diligence is applied holistically, categorization of any particular measure is not essential.

87. Koivurova, *supra* note 37; *see also* Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, *in* Report of the International Law Commission A/56/10, at 153 (art. 3 cmt. 3) (2001).

standard has been enforced in other contexts.[88] Hungary violated the Convention on the Elimination of All Forms of Discrimination against Women when it failed to "act with due diligence to prevent violations of rights or to investigate and punish acts of violence, and for providing compensation."[89] In reaching its conclusion, the committee considered three factors: lack of adequate legislation to ensure prevention of harm,[90] lack of priority given to the prosecution of violators,[91] and the failure of the state to provide information as to possible alternative avenues to ensure adequate vindication of legal rights.[92] In a case involving Brazil, the Inter-American Commission on Human Rights similarly found a "general pattern of negligence and lack of effective action by the state in prosecuting and convicting aggressors," as well as general "judicial ineffectiveness."[93] The Inter-American Court of Human Rights has also explained that it could hold states responsible for failing to punish violators and to provide victims needed assistance in recovery.[94]

Thus, in holding states responsible for failing to exercise due diligence, courts have looked holistically at each of the four areas.[95]

88. As previously mentioned, many of the cases elaborating on what the standard of due diligence requires in each of these areas arise in the context of state efforts to prevent violence against women. Others arise in the international environmental context. While all of these cases are not perfect fits for the cyber context, they provide the framework for a standard of care that is increasingly becoming customary law.

89. *Views of the Committee on the Elimination of Discrimination against Women under Article 7, Paragraph 3, of the Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women*, Comm. on the Elimination of Discrimination against Women, Rep. on its 32nd Sess., Jan. 10–28, 2005, U.N. Doc. A/60/38 (Part I), at 37 ¶ 9.2 (2005) [hereinafter A.T. v. Hungary]. The case involved a woman who had been physically abused for a period of four years. Hungarian state law was deemed inadequate to address her human rights violations.

90. *Id.* at ¶ 9.3 ("[T]he Committee notes that the State party [Hungary] has admitted . . . that legal and institutional arrangements in the State party are not yet ready to ensure the internationally expected, coordinated, comprehensive and effective protection and support for the victims of domestic violence."). Note that the committee reached this conclusion even though pending legislation might have changed the situation.

91. *Id. (*"The Committee further notes the State party's general assessment that domestic violence cases as such do not enjoy high priority in court proceedings.").

92. *Id.*

93. Maria da Penha v. Brazil, Case 12.051, Inter-Am. Comm'n H.R., Report No. 54/01, OEA/Ser./L/V/II.111, doc. 20 rev. ¶ 56 (2001).

94. Velásquez Rodríguez v. Honduras, Decisions and Judgments, Inter-Am. Ct. H.R. (ser. C) No. 4, ¶ 176 (July 29, 1988).

95. In doing so, I hope to provide an overview and bring together disparate extant strands of analysis. Such an effort is necessarily not comprehensive. Each of these areas deserves more extensive analysis than can be accomplished in this Comment.

a. Prevent

One of the most significant requirements of prevention is the responsibility to adopt laws and policies appropriate for ensuring compliance.[96] It is insufficient for a state to disclaim responsibility by relying on inadequate existing domestic laws.[97] As mentioned, in the Hungary case, the lack of "specific legislation" to combat the harm was seen as deeply problematic. The state was liable for the lack of laws even though it "instituted a comprehensive action programme against domestic violence" and a wide range of pending legislation to deal with the problem.[98] Moreover, as the Hungary example illustrates, generic criminal laws may also be inadequate. Thus, a state is required to put in "place effective criminal-law provisions to deter the commission of offenses."[99]

Likewise, in its advisory opinion on Responsibility and Liability for International Seabed Mining, the International Tribunal for the Law of the Sea provided three principles underlying obligations to prevent trans-boundary environmental harm which can also serve (with some modification) as principles for preventing against trans-boundary cyber-attacks and cybercrime: a precautionary approach, best [environmental] practices, and [environmental] impact assessments.[100]

A precautionary approach implies a proactive approach to preventing trans-boundary harm.[101] States cannot rely on uncertainty to fail to take necessary steps. Instead, states should act upon "plausible indications of potential risk."[102] Best practices would

96. U.S. v. Gr. Brit., 29 R.I.A.A. 125, 125–34 (1871), *available at http://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf*.

97. A.T. v. Hungary, *supra*, note 89.

98. *Id*.

99. Osman v. U.K. App. No. 23452/94, 1998 Eur. Ct. H.R.. *See also* Hasselbacher, *supra*, note 74; Tzevelekos, *supra* note 14.

100. Seabed Disputes Chamber of the International Tribunal for the Law of the Sea, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion (Feb. 1, 2011), *available at* https://www.itlos.org/fileadmin/itlos/documents/cases/case_no_17/adv_op_010211.pdf. Other obligations listed in the opinion are less relevant in the cyber context or specific to the Law of the Sea: "the obligation to assist the Authority in the exercise of control over activities in the Area" "the obligation to take measures to ensure the provision of guarantees in the event of an emergency order by the Authority for protection of the marine environment," and "the obligation to ensure the availability of recourse for compensation in respect of damage caused by pollution." *Id*.

101. *Id*.

102. *Id*. ¶ 131.

require states to use the "best technology available" in developing and implementing protocols to prevent cyber-attacks and cybercrime.[103] Impact assessment would require that a state consider the impacts of its cyber policies and internet policies on the proliferation of cybercrime and cyber-attacks. States should also regularly evaluate their progress in preventing cybercrimes. Each of these should be a component of a state's efforts to prevent trans-boundary cybercrime.

Finally, some additional requirements for preventing trans-boundary cyber harm might include promoting research and data collection to understand the scope of the problem, and drawing up action plans.[104]

b. Protect

Due diligence requires not merely the adoption of laws, but also "a certain level of vigilance in their enforcement."[105] Even adequate legislation is insufficient if not "backed up by law-enforcement machinery for the prevention, suppression and sanctioning of breaches of such provisions."[106]

States are also required to ensure that sufficient institutional capacity exists to diligently respond to alleged crimes and effectively monitor for trans-boundary harm. In order to do so, adequate training is required to ensure that law enforcement personnel are equipped to respond to violations of the law.[107] In the cybercrime context, this might involve ensuring that there are individuals in various governmental agencies with the adequate technological training. This would also include conducting official investigations in response to alleged violations.[108]

Another component of both prevention and protection would involve co-operation with other states in response to acts causing trans-boundary harm. In the *Pulp Mills* judgment, a dispute between Argentina and Uruguay over construction on the Uruguay River, the

103. *Id.*

104. UNECE, *Convention of the Transboundary Effects of Industrial Accidents*, Volume 2105, I-36605 Annex IV. 4, *available at* http://www2.unitar.org/cwm/publications/cbl/synergy/pdf/cat3/unece/trans_effect_ind_accidents/convention_trans_ind_en.pdf.

105. Pulp Mills Case (Arg. v. Uru.), 2010 I.C.J. 14, ¶197 (April 20).

106. R.R. v. Hungary, 2012 Eur. Ct. H.R. 2001 at ¶ 28 (2012).

107. *Id.*

108. M.C. v. Bulgaria, 2003 Eur. Ct. H.R. 651 at ¶¶ 148–66.

ICJ explained that cooperation between the parties was "necessary in order to fulfill the obligation of prevention."[109] The Draft Articles on Prevention of Trans-boundary Harm from Hazardous Activities explains this obligation as follows: "States concerned shall cooperate in good faith and, as necessary, seek the assistance of one or more competent international organizations in preventing significant trans-boundary harm or at any event in minimizing the risk thereof."[110] Likewise, regarding international co-operation, the Palermo Convention on Transnational Organized Crime, to which Russia is a signatory, requires states to provide each other "the widest measure of mutual legal assistance."[111] States are also forbidden from refusing to provide such assistance on the ground that an offense merely "involve[s] fiscal matters."[112]

c. Prosecute

States are obligated to make prosecution of trans-boundary crimes a priority. In the aforementioned Hungary case, the court found Hungary in violation of its due diligence obligation in part because prosecutions of violence against women did "not enjoy high priority in court proceedings."[113] Commentary on the United Nations Convention on the Law of the Sea emphasizes that due diligence imposes on states a positive obligation to ensure that their legal system adequately forbids and punishes prohibited conduct.[114] The prosecution of crimes should provide sufficient deterrence to help prevent additional violations.[115]

109. Pulp Mills Case (Arg. V. Uru.), 2010 I.C.J. 14, ¶102 (April 20).

110. Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, [with commentary], *in* Report of the International Law Commission, Fifty-third Session, UN GAOR, 56th Sess., Supp. No. 10, at 148–70, U.N. DOC. A/56/10 (2001) [hereinafter Draft Articles].

111. United Nations Convention Against Transnational Organized Crime and the Protocols Thereto [hereinafter Palermo Convention], art. 18, 2004, *available at* http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

112. *Id*. at art. 16 sub. 15.

113. A.T. v. Hungary, *supra* note 89, at ¶ 9.3.

114. David Freestone, *Advisory Opinion of the Seabed Disputes Chamber of International Tribunal for the Law of the Sea on 'Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area,'* AMERICAN SOCIETY OF INT'L LAW (March 2011), *available at* http://www.asil.org/insights/volume/15/issue/7/advisory-opinion-seabed-disputes-chamber-international-tribunal-law-sea-#_ednref10.

115. *See* Osman v. U.K., *supra* note 99.

In evaluating whether prosecutions are adequate, the overall pattern of prosecutions should be considered. It is insufficient to occasionally prosecute violators; what is needed is sustained and regular enforcement and prosecution. For instance, with Brazil, the Inter-American Commission on Human Rights found that the "general pattern of negligence and lack of effective action by the state in prosecuting and convicting aggressors [of violence against women]," as well as general "judicial ineffectiveness," constituted a violation of the state's obligation.[116]

Another component of prosecutions of cybercrimes should involve developing protocols for extradition of criminals. Extradition and cooperation in prosecution have been integral to international efforts at combating cybercrime.[117] Some have argued that states are obligated by customary international law to either prosecute or extradite criminals. Zdzislaw Galicki, a member of the United Nations International Law Commission has described this as "a right recognized in international law and even considered by some jurists as *jus cogens*".[118] Thus, states should make a good faith effort to cooperate with the extradition of suspected cybercriminals.

d. Redress

States are also required to assist victims of trans-boundary harm. Of all of the state responsibilities outlined, the responsibility to provide redress is the least well-defined as a matter of customary law. In most circumstances, redress is determined based on specific agreements narrowly tailored to certain kinds of trans-boundary

116. Maria da Penha v. Brazil, Case 12.051, Inter-Am. Comm'n H.R., Rept. No. 54/01, ¶ 56, (1998).

117. *See* Andy Greenberg, *Cybercops Without Borders*, FORBES (June 1, 2009), http://www.forbes.com/2009/06/01/cyberbusts-security-internet-technology-security-cyberbusts.html; Mark Clayton, *Hacker's Extradition for Cyber Heist: Sign U.S. is Gaining in Cyber Crime Fight*, CHRISTIAN SCIENCE MONITOR (Aug. 11, 2010), http://www.csmonitor.com/USA/Justice/2010/0811/Hacker-s-extradition-for-cyber-heist-sign-US-is-gaining-in-cyber-crime-fight.

118. Zdzislaw Galicki, *The Obligation to Extradite or Prosecute ("aut dedere aut judicare") in International Law: Preliminary Remarks* (2004), *available at* http://legal.un.org/ilc/reports/2004/english/annex.pdf; *See also* AMNESTY INTERNATIONAL, INTERNATIONAL LAW COMMISSION: THE OBLIGATION TO EXTRADITE OR PROSECUTE (*AUT DEDERE AUT JUDICARE* (2009), *available at* http://www.amnesty.org/en/library/asset/IOR40/001/2009/en/a4761626-f20a-11dd-855f-392123cb5f06/ior400012009en.pdf

harm.[119] However, there are ongoing efforts to develop articles on state liability for damages to supplement the ILC's articles on State Responsibility,[120] and scholars have attempted to elaborate on state responsibility to offer redress.[121]

Some have suggested that states can fulfill their responsibility to provide redress in numerous ways. A state could follow a minimalist "access to justice" approach,[122] which would allow non-state actors full access to courts and the recourse of national laws.[123] The courts would have to have "necessary jurisdiction and competence."[124] The civil law of a state should allow victims to sue and recover damages.[125]

Alternatively, a state could offer a "compensation approach" to providing redress by offering direct aid to those that suffer as a result of trans-boundary harm.[126] This compensation could take on a variety of different forms. For instance, the Draft Principles on the Allocation of Loss suggests that states could require the establishment of "industry-wide funds at the national level."[127] Other forms of compensation might rely on public or private insurance.[128]

Regardless of the approach taken, the non-discrimination principle would govern all efforts to provide redress.[129] States would be required to offer the same level of assistance in helping trans-boundary victims as they do to their own nationals. The Draft Principles on the Allocation of Loss also suggest that international

119. Worku Damena Yifru, Kathryn Garforth & Paola Sacrone, *Review of Issues, Instruments and Practices Relevant to Liability and Redress for Damage Resulting from Transboundary Movement of Living Modified Organisms*, SECRETARIAT OF THE CONVENTION ON BIOLOGICAL DIVERSITY (2012), *available at* http://bch.cbd.int/protocol/cpb_technicalseries/cpb-ts-03-en.pdf.

120. Draft Principles on the Allocation of Loss in the case of Transboundary Harm Arising out of Hazardous Activities [hereinafter Draft Principles on the Allocation of Loss], UN General Assembly Resolution 61/36 ANNEX, UN DOC. A/RES/61/36 (18 Dec. 2006).

121. A.E. Boyle, *Globalising Environmental Liability: The Interplay of National and International Law*, 17 J. ENV. L. 3 (2005); *see also* Caroline Foster, *The ILC Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities*, 14 RECIEL (3) (2005).

122. Boyle, *supra* note 121, at 9.

123. *Id*.

124. Draft Principles on the Allocation of Loss, *supra* note 120.

125. *Id*.

126. Boyle, *supra* note 121.

127. Draft Principles on the Allocation of Loss, *supra* note 120.

128. *Id*. at Principle 4.

129. Boyle, *supra* note 121.

cooperation should be an integral component of redress efforts.[130] The state is expected to "consult with and seek the cooperation of all States affected or likely to be affected to mitigate the effects of transboundary damage."[131]

In addition, redress should be "prompt and adequate." The ILC in its comment on the Draft Principles of the Allocation of Loss based this standard on the *Trail Smelter* decision arguing that "the basic principle established in that case entailed a duty of a State to ensure payment of prompt and adequate compensation for any transboundary damage."[132] In the accompanying commentary, this standard was elaborated upon to mean compensation that is "predictable, equitable, expeditious and cost effective."[133] While there is ongoing debate as to whether this is a "soft law" principle, or an obligatory element,[134] it is at the very least an emerging international norm.[135]

In the cyber-law context, under an access of justice approach states would be required to allow for either effective civil litigation against those that perpetuate cyber-attacks or offer direct compensation as part of criminal prosecution. A compensation approach could take on a variety of forms. A state might help to rebuild or repair sites that are taken down by cyber-attacks. States might also offer compensation for time that a site is down as a result of cyber-attacks or other forms of economic redress. Either of these approaches, if undertaken with adequate diligence, could meet a state's international obligation to provide redress.

IV. RUSSIA AS A PARTY TO INTERNATIONAL AGREEMENTS

In addition to Russia's basic obligation of due diligence, Russia is a signatory to international agreements that further solidify its responsibility to combat organized cybercrime.[136] In May 2004, Russia

130. Draft Principles on the Allocation of Loss, *supra* note 120, at Principle 6.

131. *Id*. at Principle 5.

132. Report of the International Law Commission, Fifty-Sixth Session, 197 (May–Aug. 2004).

133. *Id*. at 185.

134. The ILC suggests that compensation might be obligatory ("the basic principle established in that case entailed a duty of state to ensure payment of prompt and adequate compensation for any transboundary damage."). *Id*. at 197.

135. Boyle, *supra* note 121, at 17.

136. Committee of Experts on Terrorism, *Cyberterrorism – The Use of the Internet for Terrorist Purposes, Russian Federation* (Oct. 2007), *available at* http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Russian%20Federation.pdf.

signed on to the United Nations Convention against Transnational Organized Crime (also called the Palermo convention because it was signed in Palermo, Italy).[137] Signatories committed to create laws necessary to criminalize and punish not just illegal criminal activities of organized groups, but also conspiracies in such organized groups.[138] The convention also requires states to ensure that bribery and corruption are adequately punished and to "adopt legislative, administrative, or other effective measures to promote integrity and to prevent, detect, and punish the corruption of public officials."[139] Article 13 of the convention also requires states to cooperate to prevent trans-boundary criminal activity and to respond by taking measures to "identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities . . . ."[140] Signatory states are also bound to provide each other with "the widest measure of mutual legal assistance," and states cannot refuse to provide such assistance on the ground that an offense merely "involve[s] fiscal matters."[141] Another relevant provision requires states to take measures to encourage those that have participated in the criminal activities of organized groups to cooperate with the authorities.[142]

On the other hand, Russia has refused to sign the Council of Europe Convention on Cybercrime (Budapest Convention). Publically, Russia has justified its objections by pointing to provisions of the convention dealing with unilateral trans-border access of computer data, which it claims would violate its sovereignty.[143] However, some have argued that Russia's refusal to sign really stems

137. United Nations Convention against Transnational Organized Crime, (Status as of June 12, 2014). available at https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&lang=en. The Palermo Convention defines "Organized criminal group" as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit[.]" Palermo Convention, *supra* note 111, at Article 2, (a).

138. Palermo Convention, *supra* note 111, at Article 6(1)(b)(ii).

139. *Id*. at Article 9(1).

140. *Id*. at Article 13(2).

141. *Id*. at Article 18(1).

142. *Id*. at Article 26.

143. Maria Lewytzkyj, *Tactics in Cybersecurity: Russia & US – Don't Forget the Council of Europe Cyber-Crime Convention*, EXAMINER.COM (July 1, 2009), http://www.examiner.com/article/tactics-cybersecurity-russia-us-don-t-forget-the-council-of-europe-cyber-crime-convention.

from an unwillingness to take upon itself "an obligation to assist other nations in cybercrime investigations given the numerous cyber-attacks that emanate from Russia."[144]

Russia's alternative proposal instead focuses on restricting internet conduct "aimed at undermining the political, economic, and social system of another government."[145] However, Russia's proposal does not create any rules governing state responsibility to prevent and respond to cyber-attacks. Russian efforts have also been criticized for their focus on suppressing the free flow of information and resorting to excessive censorship.[146]

Despite Russia's refusal to sign on to the Budapest convention, the Palermo Convention still obligates Russia to work diligently to eradicate organized crime and associated corruption, which coincidently includes cybercrime.

V. RUSSIAN EFFORTS TO COMBAT THE MAFIA AND CYBERCRIME: HALTING SUCCESS AMIDST FAILURE

In Russia, organized crime has long proliferated. While Russia has made great strides in combating the Mafia in some areas, the government's efforts seem to have led the Mafia to more heavily involve itself in cybercrime and particularly trans-boundary cybercrime.[147]

The factors contributing to the growth of the Mafia have been thoroughly studied.[148] In the late 1980s and 1990s, government efforts to transition to a market economy without a legal structure

144. Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 207, 218 (Nat'l Research Council ed., 2010).

145. *See* Daniel Kennedy, *Deciphering Russia: Russia's Perspectives on Internet Policy and Governance*, GLOBAL PARTNERS DIGITAL 9–10 (Nov. 18, 2013), http://www.gp-digital.org/wp-content/uploads/pubs/FINAL%20-%20Deciphering%20Russia.pdf.

146. Avner Levin, *Securing Cyberspace: A Comparative Review of Stratagies Worldwide*, TED ROGERS SCH. OF MGMT. - RYERSON U. 36 (July 2012), http://www.ryerson.ca/content/dam/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf.

147. For an overview of the Mafia's shift from violent crime to blue-collar crime, *see generally* Vsevolod Sokolov, *From Guns to Briefcases: The Evolution of Russian Organized Crime*, 21 WORLD POL'Y J. 68, 72 (2004). *See also* Dan Kaplan, *Russian Cyber Crime Market More* Organized, Lucrative, SC MAGAZINE (April 24, 2012), *available at* http://www.scmagazine.com/russian-cyber-crime-market-more-organized-lucrative/article/238100/ (describing the shift from a disorganized cyber crime underground to an organized and professionalized endeavor led by the Russian Mafia).

148. *See, e.g.*, Sokolov, *supra* note 147; *see also* James Ruth, *The Russian Mob: Organized Crime in a Fledgling Democracy*, AUBURN U., http://www.auburn.edu/~mitrege/FLRU2520/RussianOrganizedCrime.htm (last visited Sept. 19, 2014).

ready to enforce "transparency, accountability, and shareholders' rights" proved fertile grounds for the growth of illicit activities.[149] Poverty and unemployment led many to become involved in organized crime organizations.[150] Corrupt police officers accepted bribes and "looked the other way" as the Mafia engaged in criminal activity without fear of punishment.[151] Judicial prosecutions failed to target high-level mafia officials, and even when small-time criminals were prosecuted, these criminals rarely faced jail time.[152] The Mafia also manipulated the judicial system by various means such as bringing prosecutions in order to sabotage business competitors.[153] Indeed, the legal situation in Russia has been described as "legal nihilism."[154] In fact, in 2008, President Vladimir Putin acknowledged that fighting against corruption was "the most wearying and difficult (problem) to resolve."[155]

While Russia has spoken about the importance of combating "legal nihilism," its rhetoric has mostly been followed by inaction.[156] Indeed, despite rhetoric opposing the actions of organized groups, the Russian Government has been accused of using organized crime to do "whatever the government of Russia cannot acceptably do as a government[,]" including criminal operations such as arms trafficking.[157] Some have even suggested that Russia is virtually a "mafia state."[158]

149. *Id*.

150. *Id*.

151. *Id*.

152. *Id*. *See also* Williams *infra* note 225 and accompanying text.

153. Thomas Firestone, *Armed Injustice: Abuse of the Law and Complex Crime in Post-Soviet Russia*, 38 DENV. J. INT'L L. & POL'Y 555, 571 (2009–2010).

154. E. K. Matevosova, *Legal Nihilism in Russia and Its Causes*, 2011 CURRENT ISSUES RUSS. L. 22 (2011); *see also* Kathryn Hendley, *Who are the Legal Nihlists in Russia?*, 28 POST-SOVIET AFF. 149 (2012).

155. Vladimir Putin, President of Russ., Remarks at Annual Big Press Conference (Feb. 14, 2008) (transcript available at http://archive.kremlin.ru/eng/speeches/2008/02/14/1011_type82915_160266.shtml).

156. John Barham, *Russia's Cybercrime Haven*, SECURITY MGMT. (Nov. 1, 2008), https://sm.asisonline.org/Pages/Russias-Cybercrime-Haven.aspx.

157. Luke Harding, *WikiLeaks Cables: Russian Government 'Using Mafia for its Dirty Work'*, GUARDIAN (Dec. 1, 2010), http://www.theguardian.com/world/2010/dec/01/wikileaks-cable-spain-russian-mafia.

158. *Russia is Virtual 'Mafia State,' Says Spanish Investigator*, GUARDIAN (Dec. 2, 2010), http://www.theguardian.com/world/us-embassy-cables-documents/247712.

Despite these problems, some positive steps have been taken, including efforts to root out corruption in the police force.[159] Likewise, state efforts to stop money laundering by organized crime have been seen as very successful.[160] Russia has also enacted several strong laws targeting corruption and money laundering,[161] and prosecuted thousands of cases of corruption.[162] One leading study also suggested that the so-called "bribe tax" declined between 2002 and 2005,[163] but the results have been mixed, as other studies suggest a steady growth in bribes that exceeds the rate of inflation.[164] Yet, other studies have measured an increase of overall corruption.[165] And regardless, it is nearly impossible to overstate how pervasive corruption continues to be,[166] and Russian citizens continue to

159. *Government Flexes Legal Muscle in Corruption in Russia Fight*, THINK RUSSIA (June 17, 2010), http://www.thinkrussia.com/policy-initiatives/government-flexes-legal-muscle-corruption-russia-fight.

160. *See Anti Money-Laundering Law is Enacted in Russia*, PRICEWATERHOUSECOOPERS TAX AND LEGAL FLASH REPORT (July 2013), *available at* http://www.pwc.ru/en/tax-consulting-services/legislation/assets/tax-flash-report-issue-24-342-eng.pdf; *but see* Alexandra V. Orlova, *Russia's Anti-Money Laundering Regime: Law Enforcement Tool or Instrument of Domestic Control?*, 11 J. MONEY LAUNDERING CONTROL 210 (2008).

161. *See* William D. Semins & Denise N. Yasinow, *Russia Amends Anti-Corruption Law to Require Affirmative Anti-Corruption Compliance Measures*, K & L GATES (May 8, 2013), http://www.klgates.com/files/Publication/6e522369-093b-4d2d-bc07-005d0fbb0860/Presentation/PublicationAttachment/3ca1d514-2937-4523-bda1-03388b86bbec/Government_Enforcement_Alert_05022013.pdf.

162. In the first ten months of 2007 alone, 8,500 officials were charged and over 37,000 cases of corruption were uncovered. *8,500 Russians Charged with Corruption: Official*, EDMONTON J. (Nov. 22, 2007), at A4, http://www.canada.com/story.html?id=d0c04854-743d-4f1e-8337-e7011423a2ab.

163. Michael Alexeev & Robert Conrad, *Assessment of Tax Reform Results in Russia: Comparative Analysis* 11 (Gaidar Inst. for Econ. Policy, Working Paper No. 0001, 2009), *available at* http://www.iep.ru/files/RePEc/gai/wpaper/0001Alexeev-Conrad.pdf.

164. *See* Alexandra Kalinina, *Corruption in Russia as a Business*, INSTITUTE OF MODERN RUSSIA (Jan. 2013), http://imrussia.org/en/society/376-corruption-in-russia-as-a-business. In addition, a team from the World Bank recently noted that those companies that are required to pay a bribe are increasingly expected to pay more. WORLD BANK, POLICY NOTE: RUSSIAN FEDERATION: NATIONAL AND REGIONAL TRENDS IN REGULATORY BURDEN AND CORRUPTION 5 (Feb. 2013), *available at* http://www.worldbank.org/content/dam/Worldbank/document/eca/Russia-Regional-BEEPS-2013.pdf.

165. Terry Miller et al., *Index of Economic Freedom: Russia*, HERITAGE FOUND. 365–66 (2014), http://www.heritage.org/index/pdf/2014/countries/russia.pdf.

166. PHILIP GOUNEV & TIHOMIR BEZLOV, CTR. FOR THE STUDY OF DEMOCRACY, EXAMINING THE LINKS BETWEEN ORGANISED CRIME AND CORRUPTION 303–04 (2010), *available at* http://ec.europa.eu/dgs/home-affairs/doc_centre/crime/docs/study_on_links_between_organised_crime_and_corruption_en.pdf.

express pessimism at the possibility of stopping corruption.[167] Thus, there have been some encouraging steps, but corruption remains an immense problem.

Moreover, the government's increased efforts to stamp out money laundering and other lucrative efforts of criminal enterprise have forced Russian organized crime to adopt new methods and tactics.[168] Cybercrime seems to be one of the new enterprises that have replaced traditional Mafia activities. Russian cybercrime activities have evolved into some of the most complex in the world and malware produced by former soviet countries, including Russia, has "been dubbed the 'Faberge Egg[]' of the malware world," due to its elegance and sophistication.[169] Russia has failed to take action to shut down cybercrime groups, even amidst public attention and pressure. For example, the Russian Business Network (RBN), a group engaged in a multitude of cybercrimes, including child pornography and identity theft, was shut down only after international internet service providers began to aggressively pursue them.[170] There have been a couple instances of the Russian authorities arresting cybercriminals, but these cases have led to limited jail time and are unlikely to serve as an adequate deterrent to criminals.[171]

As the next section will show, Russia has made some limited progress in recent years. However, its current efforts fall far short of what would be expected of it under the standard of due diligence.

167. Ivan Nechepurenko, *Russians Lose Hope that State Can Tackle Corruption, Transparency Says*, MOSCOW TIMES (July 10, 2013), http://www.themoscowtimes.com/news/article/russians-lose-hope-that-state-can-tackle-corruption-transparency-says/482941.html.

168. Sokolov, *supra* note 147.

169. Tom Kellermann, *Peter the Great Versus Sun Tzu*, TREND MICRO (Sept. 2012), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/op_kellermann_peter-the-great-vs-sun-tzu.pdf (discussing differences between Russian and Chinese cybercrime groups).

170. John Barham, *Russian Cybercrooks Adopt Lower Profile*, SECURITY MGMT. (Apr. 1, 2008), *available at* https://sm.asisonline.org/Pages/Russian-Cybercrooks-Adopt-Lower-Profile.aspx. Russia was repeatedly asked to coordinate in the fight against the RBN and refused to do so. *See* Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, WASHINGTON POST (Oct. 13, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html?sid=ST2007101202661.

171. Robert Lipovsky et al., *Cybercrime in Russia: Trends and Issues*, ESET (2011), http://www.eset.com/us/resources/white-papers/CARO_2011.pdf.

VI. RUSSIA IS FALLING FAR SHORT OF ITS DUE DILIGENCE OBLIGATIONS

Russia has taken some positive steps to combat cybercrime. However, its current efforts still fall short of the international requirements of due diligence. The following sections will examine Russia's failure to fulfill the specific component of due diligence. First, Russian cybercrime causes trans-boundary cybercrime. Second, Russia should be held to a high level of due diligence. Third, Russia has fallen short of its due diligence obligation to prevent, protect, prosecute, and redress cybercrime.

A. Russian Cybercrime Causes Trans-boundary Harm

Much of the cybercrime occurring in Russia clearly meets the international standard for trans-boundary harm.[172] First, cybercrime is clearly a result of human activity. Second, the Russian cybercrime groups are primarily utilizing Russian cyber-infrastructure including IP addresses to launch cyber-attacks.[173] Thus, Russia is expected to exercise due diligence to monitor and prevent these trans-boundary activities.

Additionally, the activities of cybercriminals and the Russian Mafia are clearly capable of giving rise to harm. With an economic toll of hundreds of millions or even billions of dollars annually, it is clear that on the aggregate these crimes rise to the level of "significant" or even "serious" harm. And a significant portion of the cybercrime emanating from Russia could also be classified as having physical consequences.[174] Finally, a significant portion of the harm caused by the Russian Mafia impacts individuals or objects, such as computers or computer networks, located in other countries.[175] Thus, the harm caused by the Russian Mafia and Russian organized crime rises to the level of trans-boundary harm and is sufficient to trigger Russia's obligation to exercise due diligence in preventing, protecting against, prosecuting, and redressing transnational cybercrime.

172. *See* Ilaşcu v. Moldova, 2004 Eur. Ct. H.R., 318 at ¶ 331.

173. For instance, all of the cyber attacks against Georgia were traced to Russian-based servers. *See* Tom Espiner, *Georga Accuses Russia of Coordinated Cyberattack*, CNET (Aug. 2008), http://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/.

174. *See supra* notes 57–62 and accompanying text.

175. *See* Casaretto, *supra* note 5.

B. The Degree of Diligence Expected of Russia

The next question is in regard to the level of reasonableness or diligence to be expected of Russia. There is a strong case to be made that Russia should be held to a very high level of due diligence in regard to organized cybercrime.

First, Russia has large financial resources and has shown a capacity to engage in projects of a large scale.[176] Second, in terms of technological resources, Russia is considered one of the most technologically advanced countries in the world.[177] Among similarly situated members of BRICS,[178] Russia has been ranked as having far greater technological development.[179] Russia is also notorious for having some of the most advanced military technology,[180] and has even utilized hacking and other cyber activities in warfare.[181] Thus, Russia is technologically well situated to wage a vigorous effort against cybercrime.

Moreover, the Russian federal government has under presidents Putin and Medvedev increasingly centralized power.[182] This includes

176. For instance, in 2014, the country hosted the most expensive Olympic games of all time. Although of course, the resources needed to engage in a protracted conflict against cyber criminals is different than those needed to build an Olympic stadium. Adam Taylor, *Why Sochi Is By Far the Most Expensive Olympics Ever*, BUS. INSIDER (Jan. 17. 2014), http://www.businessinsider.com/why-sochi-is-by-far-the-most-expensive-olympics-ever-2014-1.

177. Kenneth Rapoza, *Russia's High Tech Promise*, FORBES (Aug. 22, 2011), http://www.forbes.com/sites/kenrapoza/2011/08/22/russias-high-tech-promise/; Andrew E. Kramer, *Russia Takes Big Step into Technology*, N.Y. TIMES (May 25, 2010), http://www.nytimes.com/2010/05/26/business/global/26ruble.html?_r=0.

178. The term BRICS refers to Brazil, Russia, India and China and was coined by economist Jim O'Neill. *See Information about BRICS,* BRICS, *available at* http://brics6.itamaraty.gov.br/about-brics/information-about-brics (last visited Sept. 26, 2015).

179. Joshua Keating, *The Most Wired Country in the World is . . .*, FOREIGN POL'Y, (Apr. 12, 2013) , *available at* http://ideas.foreignpolicy.com/posts/2013/04/12/the_most_wired_country_in_the_world_is.

180. Mark Galeotti, *Russia's Shiny New Toys*, OPEN DEMOCRACY, (Jan. 10, 2014), *available at* http://www.opendemocracy.net/od-russia/mark-galeotti/russia%E2%80%99s-shiny-new-weapons; *Russian Military Hardware Best in the World*, PRAVDA, Dec. 19, 2012, http://english.pravda.ru/russia/economics/19-12-2012/123231-russia_military_hardware-0/.

181. *See* Isaac R. Porche III, *Cyberwarfare Goes Wireless*, U.S. NEWS (April 4, 2014), *available* at, http://www.usnews.com/opinion/blogs/world-report/2014/04/04/russia-hacks-a-us-drone-in-crimea-as-cyberwarfare-has-gone-wireless.

182. Paul Goble, *New Regional Policy Draft Pushing Russia Toward Hyper-Centralized 'Post-Federalism,' Shtepa Says*, THE INTERPRETER, (June 1, 2015) http://www.interpretermag.com/new-regional-policy-draft-pushing-russia-toward-hyper-centralized-post-federalism-shtepa-says/; Peter Baker, *Putin Moves to Centralize Authority*, WASH. POST, Sept. 14, 2004, *available at* http://www.washingtonpost.com/wp-

state control of television and radio stations with President Putin recently dissolving one of the main state news agencies in order to create a television network focused on promoting a positive image of Russia.[183] The Russian government has also heavily censored the internet and prosecuted journalists and bloggers for publishing "extremist" material.[184] Russia's efforts to censor and suppress extremist literature and block websites critical of the government evidence a great capacity to control and regulate internet activity.[185]

Despite the margin of appreciation that is granted to states in attempting to institute unique policies and respond to state specific challenges,[186] Russia's attempts to censor internet speech and discourse cannot be credited as an effort to control cybercrime. As I have argued elsewhere, Russia's laws are or should be considered a violation of the European Convention of Human Rights and a violation of both Freedom of Expression and Freedom of Conscience.[187] Moreover, there is evidence of cyber-attacks (possibility state sponsored) being used as a tool to suppress opposition voices on the internet.[188] Thus, Russia's speech-suppressing policies actually lead to the proliferation rather than the cessation of cybercrime and cyber-attacks.

The seriousness of cybercrime being committed by Russians would require Russia to exercise a great degree of diligence. The economic harm caused by the cyber-attacks is significant, but other

dyn/articles/A17838-2004Sep13.html.

183. Timothy Heritage, *Putin Dissolves State News Agency, Tightens Grip on Russia Media*, REUTERS, (Dec. 9, 2013), *available at* http://www.reuters.com/article/2013/12/09/us-russia-media-idUSBRE9B80I120131209.

184. *See* Draft Articles, *supra* note 110.

185. RIA NOVOSTI, *Russian Media is Instrument of State Control*, SPUTNIK (Apr. 12, 2011), http://en.ria.ru/russia/20110412/163492415.html.

186. Another limitation on Russia's ability to act is the fact that a not insubstantial portion of cybercrime comes from Chechen or other ethnic groups. Efforts to combat such groups may be fraught with ethnic and geo-political tension. On the other hand, Russia's invasion of Georgia in 2007 and current occupation of Crimea displays a Russian willingness to take aggressive action when its national interests or citizens are in jeopardy. Thus, Russia can be expected to likewise exercise diligence to combat cybercrime stemming from contested or occupied territory.

187. Daniel Ortner, Note, *Conscientious Offenders: Russia's Ban on 'Extremist' Religious Literature, and the European Court of Human Rights*, 56 VA. J. INT'L L. (forthcoming Oct. 2015).

188. Brigitte Hopstad, *The Russian Media Under Putin and Medvedev: Controlled Media in an Authoritarian System* (Feb. 2011) (unpublished master's thesis, Norwegian University of Science and Technology), *available at* https://www.academia.edu/979916/The_Russian_media_under_Putin_and_Medvedev_Controlled_media_in_an_authoritarian_system.

potential harm might be even more serious. Hacking tools in Russia are freely sold to any that wish to pay.[189] Such technology and equipment, if not prevented, could easily be used to commit acts of terrorism or destruction.[190]

C. Russia and the Obligation to Prevent Trans-boundary Cybercrime

Having established that Russia would be held to a high standard of care, it will now be shown that for each of the four categories—prevention, protection, prosecution, and redress—Russia's current efforts fall short.

On a broad level, it is worth noting the Information Security Doctrine of the Russian Federation, which sets out Russia's cyber policies.[191] The doctrine recognizes several flaws in current Russian cyber-security such as judicial corruption and lack of adequate laws.[192] Unfortunately, the doctrine is lacking in specific suggestions and also focuses heavily on controlling information through censorship and counter-propaganda.[193] Given its vagueness and the lack of concrete proposals, this doctrine is ill-equipped for dealing with the growing trans-boundary threat of organized cybercrime.

1. Prevention

Currently, Russia is not exerting due diligence to prevent the occurrence of cybercrime. One of the problems with Russia's efforts to fight cybercrime has been its reactive rather than proactive nature.[194] Money is spent on surveillance efforts or on attempts to

189. Carlton Purvis, *Hacking Tools Fuel Russian Black Market*, SECURITY MGMT. (Nov. 7, 2012), http://www.securitymanagement.com/news/hacking-tools-fuel-russian-black-market-0010836.

190. Such has happened with traditional military hardware. *See* Thomas Land, *Islamic Terrorists and the Russian Mafia*, 282 CONTEMP. REV. 264 (2003).

191. INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION (Approved Sept. 9, 2000), *available at* http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

192. IAN LEIGH, INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION, *available at* http://www.dcaf.ch/content/download/36442/528101/file/Doctrine_security_LEIGH.pdf

193. *Id.*

194. Indeed, this has been a common criticism of the approach of governments world-wide. *See Governments Spend too much on Cyber Surveillance and not Enough on Catching Crooks*, INFO SECURITY, June 18, 2012, *available at* http://www.infosecurity-

install anti-virus or anti-phishing tools to the exclusion of efforts to prevent actual attacks or arrest perpetrators.[195] Yet, cybercrime experts argue that such an approach is ineffective and far too slow to respond to the instantaneous nature of cybercrime.[196] Legislation criminalizing cybercrimes exists; however, as will be mentioned in the section on prosecutions, penalties may be too low to deter cybercrime. Existing laws also contain ambiguities that make them ineffective and inadequate.

Currently, there are no state sponsored agencies conducting evaluations or assessments of security standards or measuring the effects of cybercrime. The government has been productively involved with the qualitative work of security organizations such as Group-IB.[197] Nevertheless, the government should independently seek to measure and evaluate its progress by conducting impact assessments.[198]

International cooperation is another area where greater Russian effort is needed in order to meet the due diligence requirement of prevention. As already mentioned, Russia has voiced concerns over the European Convention on Cybercrime and has been unwilling to sign in part because of the fear that it will compromise "national sovereignty."[199] Russia has at times been reluctant to cooperate with international extradition efforts. However, this is an area in which Russia has a special treaty obligation; the Palermo Convention on Transnational Organized Crime, to which Russia is a signatory, urges states to "seek to conclude bilateral and multilateral agreements or arrangements to carry out or enhance the effectiveness of extradition."[200]

Russia has worked with other nations to combat cybercrime. For instance, in the case of Viacheslav Ivankov, a high-level individual in the Russian Mafia, Russian cooperation led to Ivankov's arrest and

magazine.com/view/26387/governments-spend-too-much-on-cyber-surveillance-and-not-enough-on-catching-crooks/.

195. *Id.*

196. *Anti-Virus Software Sucks Up Too Much Security Cash Claims Study*, BBC NEWS (June 18, 2012), http://www.bbc.com/news/technology-18456607.

197. GROUP IB, STATE AND TRENDS OF THE 'RUSSIAN' COMPUTER CRIME MARKET IN 2010, *available at* https://s3.amazonaws.com/hsnnetwork/pdf/russian-cybercrime-market.pdf.

198. *See supra* note 100 and accompanying text.

199. *Putin Defies Convention on Cybercrime*, C-NEWS (Mar. 27, 2008) http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913.

200. Palermo Convention, *supra* note 111, at art. 16, sub. 17.

conviction in a U.S. court.[201] Likewise, cybercriminals have been arrested as a result of transnational cooperation.[202]

On the other hand, Russia has been highly critical of American efforts to extradite Russian citizens.[203] Russia also refused to offer assistance to Estonia following the very costly cyber-attacks that crippled the state's cyber infrastructure, even though Estonia submitted a request for bilateral investigation under the Mutual Legal Assistance Treaty (MALT).[204] This refusal has been criticized as a violation of both international norms and Russia's direct treaty obligations.[205]

2. Protection

Russia has taken some steps to facilitate the work of security agencies. There is currently a website on which individuals can report cybercrimes which have been committed or are being planned or prepared.[206] There is also a Federal Security Service (FSB) e-mail address and phone number for reporting crimes.[207] Russia has also worked to develop new technologies to help agencies combat cybercrime.[208]

However, these efforts do not seem to be highly effective. For instance, of 900 reported instances of the misuse of telecommunications networks for extremist or terrorist purposes, only about 100 of the instances were responded to and stopped.[209]

201. Selwyn Raab, *Reputed Russian Crime Chief Arrested*, N. Y. TIMES, June 9, 1995, *available at* http://www.nytimes.com/1995/06/09/nyregion/reputed-russian-crime-chief-arrested.html.

202. FIGHTING RUSSIAN CYBERCRIME MOBSTERS: REPORT FROM THE TRENCHES, *available at* http://www.blackhat.com/presentations/bh-usa-09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf.

203. *See Moscow Slams Hacker's Extradition to U.S.*, RIA NOVOSTI, (Jan. 19, 2012), http://en.ria.ru/russia/20120119/170850006.html; *U.S. Admits Delay in Informing Russia of Hacker's Extradition*, RIA NOVOSTI (Jan. 20, 2012), http://en.ria.ru/russia/20120120/170855620.html.

204. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber-attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009), *available at* http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7.

205. *Id.*

206. Committee of Experts on Terrorism, *supra* note 136.

207. *Id.*

208. Oscar Williams-Grut, *The Lab Fighting Cybercrime: Russia's Weapon in the War Against Hi-tech Gangs*, INDEPENDENT July 27, 2013, *available at* http://www.independent.co.uk/news/business/analysis-and-features/the-lab-fighting-cybercrime-russias-weapon-in-the-war-against-hitech-gangs-8734594.html.

209. Committee of Experts on Terrorism, *supra* note 129.

The Federation Council of Russia held a meeting to address gaps in Russia's cyber security, and acknowledged the lack of clear incident response models to respond to cyber incidents.[210] Current security standards also fall short of recognized best practices.[211]

In order to catch individuals involved with organized cybercrime, Russia should ensure that federal crime fighting organizations such as the FSB are involved.[212] Doing so is necessary to reduce the possibility of corruption, which is more prevalent on the regional level.[213] If efforts are left to the regional police, the high levels of corruption and mafia penetration are likely to limit prosecution to merely unaffiliated or rouge individuals. However, because even high profile individuals working for the Federal Government may be subject to corruption,[214] it is also important to ensure some level of redundancy and oversight.

In order to protect against cybercrime, Russia will likely have to invest more time and resources into training experts.[215] As organized crime continues to devote more money and energy to hiring high-quality information technology specialists, the government will have to do likewise in order to catch up with organized crime.[216] Likewise, experts have recommended that Russia increase its training to "judicial, prosecutorial, investigative, and law enforcement

210. Benjamin Volcsko, *Russia Crowdsourcing It's Cyber Security Strategy: Clever Experiment or Solicitation of Internet Restriction Freedoms?*, MONETARY CYBER SECURITY INITIATIVE, *available at* http://sites.miis.edu/cysec/2014/01/20/russias-crowdsourcing-experiment-getting-the-peoples-opinion-on-the-new-cyber-security-strategy/.

211. *Id.*

212. There is currently legislation pending in the Duma to grant the FSB greater ability to respond to cybercrime. *See Russian Government Calls for FSB to Tackle Cyber Crime*, RIA NOVOSTI (Oct. 17, 2013), http://en.ria.ru/russia/20131017/184204651/Russian-Government-Calls-for-FSB-to-Tackle-Cyber-Crime.html.

213. The criminalization of the Russian Security Aparatus is well-documented. Stephen McCombie, Josef Pieprzyk & Paul Watters, *Cybercrime Attribution: An Eastern European Case Study*, PROCEEDINGS OF THE 7TH AUSTRALIAN DIGITAL FORENSICS CONFERENCE (December 3, 2009).

214. An officer of the Russian Interior Ministry's K Directorate, which investigates cybercrimes, was arrested and charged with corruption in 2012. *Officer of Russian IT Directorate Arrested*, RADIO FREE EUROPE (April 24, 2012), http://www.rferl.org/content/russian_cybercrime_officer_arrested/24558486.html.

215. *See* John Leyden, *Russian Cops Lack Kit to Fight Cybercrooks, Says Brit Security Buff*, THE REGISTER (June 6, 2013), http://www.theregister.co.uk/Print/2013/06/06/private_sector_leading_russian_cybercrime_cleanup/.

216. LOUISE I. SHELLEY, ORGANIZED CRIME, TERRORISM AND CYBERCRIME, 303–12 (Alan Bryden & Philipp Fluri eds., 2003), *available at* http://www.lake-project.net/download/Germany/Security/Organized%20Crime,%20Terrorism%20and%20Cybercrime.pdf.

agencies."[217] Training on the user end should also be a state priority to help reduce incidents of cybercrime.[218] Currently, no systematic programs exist to conduct this training.

Involvement of private groups may also be critical in overcoming cybercrime. In 2003, Group-IB, a public company dedicated to digital crime investigation and computer forensic consulting, was established.[219] Since establishment, Group-IB has assisted in the arrest of several criminals.[220] Since 2012, there was a marked decrease in some parts of the Russian cybercrime market, in part as a result of the group's efforts.[221] Thus, the Russian Government's involvement with the efforts of such private organizations to help protect against cybercrime represents one of the most promising signs of progress. Nevertheless, current levels of engagement with the private sector on matters of security remain low, and Russia is overall not doing enough to protect against cybercrime.

3. Prosecution

Russia's work with Group-IB to catch cybercriminals is commendable and seems to signal a shift towards greater efforts at prevention of cybercrime and prosecution of offenders of such crimes.[222] However, it is unclear whether these efforts have been successful in targeting organized crime groups rather than individual or "rogue" hackers. Russia has also prioritized domestic prosecutions to the exclusion of those causing harm to persons outside of the country. As one American cyber security expert explained, Russian "[h]ackers only really get prosecuted when they attack targets inside Russia."[223] Thus, the current legal regime perversely creates an

217. *Russian Cybercrime: What Russia is Doing, and What it Should be Doing*, INFO SECURITY (April 24, 2012), http://www.infosecurity-magazine.com/view/25359/russian-cybercrime-what-russia-is-doing-and-what-it-should-be-doing/.

218. Russia has acknowledged the importance of training citizens as part of its newest cybersecurity conception/plan. *See infra* Section VI.

219. GROUP IB, THREAT INTELLIGENCE REPORT 2012–2013, http://report2013.group-ib.com/.

220. In 2011, the group reported 10 cybercrime related arrests. *Id.*

221. *Id.* On the other hand, increased security, especially in the security sector, has led to a commensurate rise in spending on infrastructure among cybercrime groups. *See Crackdown on Cybercriminals Equals Reduced Cybercrime in Russia*, INFO SECURITY (Sept. 11, 2013), http://www.infosecurity-magazine.com/view/34472/crackdown-on-cybercriminals-equals-reduced-cybercrime-in-russia/.

222. *See* Lipovsky, *supra* note 171.

223. Ben Plesser, *Skilled, Cheap Russian Hackers Power American Cybercrime*, NBC

incentive for cybercrime groups to focus their efforts on international rather than domestic targets.

The current penalties for cybercrime are also insufficient to act as a deterrent.[224] Prior to 2011, those who committed massive trans-boundary cyber-attacks received light sentences and no jail time; for instance, two hackers who stole ten million dollars from the Bank of Scotland received only suspended sentences.[225] This was an especially glaring discrepancy given that common thieves often receive large sentences and jail time.[226] In December 2011, the Duma enacted a criminal code reform, which included aggravated circumstances leading to an increased penalty.[227] However, expert groups have criticized these steps as inadequate.[228] In particular, the statute's terminology is vague and ill-suited for responding to diverse cyber-attacks.[229] Potential profit from cybercrime still outweighs the potential risk of prosecution. Thus, current prosecutions are likely inadequate to deter the growth of cybercrime.

4. Redress

Russia has not directly adopted any known compensation schemes or efforts to assist trans-boundary victims. The Russian government has cooperated with groups, such as Group-IB, that specialize in incident response and in helping victims of cyber-attacks recover data and remove critical vulnerabilities.[230] However there is no evidence of any such efforts being directed at international victims of trans-boundary harm.

Russia has also failed to facilitate prosecutions in domestic courts. While, theoretically foreign nations have equal access to courts, in reality the court system is notoriously inaccessible to

NEWS (Feb. 5, 2014), http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371.

224. *See supra* note 115 and accompanying text.

225. Christopher Williams, *Russian Hacker Avoids Jail for $10m Royal Bank of Scotland Raid*, TELEGRAPH (Feb. 10, 2011), http://www.telegraph.co.uk/technology/news/8316246/Russian-hacker-avoids-jail-for-10m-Royal-Bank-of-Scotland-raid.html.

226. *Id*.

227. *Russian Cybercrime: What Russia is Doing, and What It Should be Doing*, *supra* note 217.

228. *Id*.

229. *Russian Cybercrime Market Doubles in Size*, HELP NET SECURITY (April 24, 2012), http://www.net-security.org/secworld.php?id=12798.

230. CERT-GIB – COMPUTER SECURITY INCIDENT RESPONSE TEAM BY GROUP-IB, http://cert-gib.com/ (last visited September 15, 2014).

foreigners.[231] Even though Russia's legal system for enforcing contracts is ranked tenth in the world,[232] rampant corruption would make private suits against individuals involved in organized crime activities especially unlikely to succeed.[233] Getting witnesses to testify against members of organized crime is difficult because witnesses are often threatened and intimidated out of testifying.[234] Thus, victims of trans-boundary cybercrime are likely out of luck in their efforts to seek compensation in the Russian court system.

In each of the categories, Russia has fallen short of its due diligence obligation. Current legislation is inadequate to prevent trans-boundary crime, police efforts are woefully uncoordinated and ineffective, prosecutions for trans-boundary cybercrime are rare and riddled with corruption, and victims lack effective avenues of redress. In order to comply with its obligations, Russia would have to pass new legislation focused on cybercrime and vigorously enforce it.

VII. CONCLUSION: FAILURE, BUT A SIGN FOR HOPE

Yet, despite its current failings, there are signs that Russia is starting to acknowledge the importance of aggressively targeting cybercrime. In 2013, the Russian Federal Council organized an investigation into potential proposals to improve cyber security. In January 2014, the group put out a draft proposal that a governmental working group will review in an effort to craft legislation.[235] These proposals would, if completely adopted and enforced, likely meet

231. Charles Clover, *Russian Court Move Seen as Power Grab*, FINANCIAL TIMES (Dec. 4, 2012), http://www.ft.com/cms/s/0/ea1bd9ac-3a0f-11e2-a00d-00144feabdc0.html.

232. International Finance Corporation, *Ease of Doing Business in Russian Federation*, WORLD BANK Group, http://www.doingbusiness.org/data/exploreeconomies/russia/#enforcing-contracts.

233. Firestone, *supra* note 153.

234. Immigration and Refugee Board of Canada, *Russia: Measures Implemented to Fight Police Corruption, including the Procedure for Filing a Complaint against the Police; the Witness Protection Program*, REFWORLD (Nov. 8, 2011), http://www.refworld.org/docid/5072b3af2.html.

235. CONCEPTION OF THE STRATEGY OF CYBERSECURITY OF THE RUSSIAN FEDERATION (in Russian) [hereinafter CONCEPTION OF THE STRATEGY OF CYBERSECURITY], *available at* http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (author's translation). For some public commentary critical of the plan, see Атаманова Г.А., *Conception of the Strategy of Cybersecurity of the Russian Federation*, АГАСОФИЯ (March 17, 2104), http://gatamanov.blogspot.com/2014/03/blog-post_17.html [Russian blog post].

Russia's due diligence obligations. The proposal addresses aspects of prevention, protection, prosecution and redress.[236]

A. Prevention

The document openly acknowledges existing gaps and seeks to increase the Russian Federation's role in cyber-security on an equal level with regional and private efforts.[237] The document calls for the systematizing of efforts and for much needed centralized coordination.[238] The government is called to work with local governments, businesses and civilian organizations in order to achieve its goals.[239] Specifically, the proposal calls for greater government interaction with the private sector including helping private companies develop better security practices.[240] Citizens would also be encouraged to propose solutions to security problems.[241] In order to encourage private involvement, the plan calls for tax subsidies and other government aid. It also calls for regular evaluations of the systems. In addition, scientific studies to analyze and research cyber security are encouraged.

The plan calls for improved legislation on cyber-security including the adaptation of international legal norms and full compliance with ratified international agreements.[242] In order to measure progress, the document recommends the development of new information security systems as well as criteria to evaluate the effectiveness of such systems.[243]

The plan also calls for the growth in international cooperation especially in regard to limiting the spread and use of "information weapons."[244] Additionally, it calls for greater interaction and information sharing between domestic and international commercial

236. Encouragingly, one "basic principle" of the plan includes free and equal access to information and knowledge. CONCEPTION OF THE STRATEGY OF CYBERSECURITY *supra* note 235 at III. 4, 3). In addition the plan mentions the need to avoid the extremes of a complete lack of security on the one hand and excessive regulation on the other. *Id*. at V 4).

237. *Id*. at III 1)–2).

238. *Id*. at VI 1).

239. *Id*. at III 3).

240. *Id*. at VI 4)–5).

241. *Id*. at VII 6).

242. *Id*. at VII 1)–2).

243. *Id*. at III 2).

244. *Id*. at III 2).

and corporate organizations.[245] The plan likewise mentions the need for greater cooperation with foreign law enforcement agencies.[246] Finally, the plan does call for the development of agreements and mechanisms to improve global cyber-security as well as a harmonization of security standards.[247]

Thus, the proposal is quite thorough in the area of prevention. It would improve international cooperation, data collection, and cooperation between state and non-state actors.[248] Such efforts would almost certainly be sufficient to satisfy due diligence.

B. Protection[249]

Importantly, the plan emphasizes that security efforts should be prioritized to focus on the most serious and likely threats to cyber security.[250] Such a priority, if implemented, would minimize many of the problems already discussed, such as the state focusing on small time criminals rather than those most heavily involved in organized cybercrime.

In addition, the proposal calls for a uniform system of technological training, as well as a one-stop portal where members of the public can go for cyber-security tools as well as information and statistics about cybercrimes.[251] The government would also seek to establish a national center to warn of cyber-threats.[252]

There is also a general call to increase the cyber-literacy of Russian citizens through a "wide spread information campaign."[253] University classes should be developed for all levels dealing with cyber issues.[254] For civil servants, knowledge of technology and cyber security would become required, and regular training would be conducted to ensure that their training remains current.[255]

245. *Id* at III 6).
246. *Id*. at VII 2).
247. *Id*. at VII 1).
248. *Id*. at III 6).
249. *Id*.
250. *Id*. at V 5)
251. *Id*. at III 2.
252. *Id*. at VI 1), VII at 5).
253. *Id*. at III 5), VII at 7).
254. *Id*. at VII 5).
255. *Id*.

The efforts at protection are also quite sweeping as they would include training of law enforcement personnel and the general public, as well as a focus on the most serious cybercrimes.[256] Such efforts would likely be sufficient to satisfy due diligence.

C. Prosecution[257]

Of all of the areas, the plan focuses the least on increasing prosecutions. Nevertheless, the plan calls for increased penalties for crimes as well as penalty enhancements for traditional crimes committed with the help of cyber technology.[258] If Russia implemented and enforced these enhanced penalties with a focus on the most serious and likely threats rather than small-time criminals, it could meet its due diligence obligation to prosecute. However, this is the one area where additional measures might be required to ensure that those most involved with organized cybercrime are prosecuted. Regardless, the proposal would be an enormous step forward.

D. Redress[259]

Redress is also not the primary focus of the plan. However, the plan calls for the development of incident response centers to detect, prevent, and eliminate the effects of cyber-attacks.[260] In addition, the government would work with insurance companies to provide risk insurance against cybercrime as well as legal assistance.[261] It is not entirely clear whether this aid would be offered to foreign companies and others injured by trans-boundary harm. However, an insurance-based model, possibly subsidized, might be an elegant and novel solution that offers aid to transnational corporations or other injured entities.[262]

256. *Id*. at VII 5).

257. *Id*.

258. *Id*. at VII 2).

259. *Id*.

260. *Id*. at VII 1).

261. *Id*. at VII 6).

262. Of course, an insurance-based model might create perverse incentives, as the Russian mafia is already heavily involved with insurance fraud and insurance related schemes. Thus, an insurance-based scheme might create an incentive for the Mafia to aggressively sell cyber-insurance and perpetuate attacks to scare businesses into making these purchases. Without adequate prosecution and deterrence, focusing on providing insurance is likely to bolster rather than stymie the Russian Mafia's conduct. *See* Jeffrey R. Hatcher, *The Russian*

The provisions of this plan are laudable and, if implemented, would likely be sufficient to ensure that Russia is in compliance with its international obligation of due diligence. This would be dependent on vigorous enforcement of the proposal as well as its application in a non-discriminatory fashion towards international organizations. It is entirely possible that such protocols would be enforced in such a way to only deter cybercrime against domestic organizations, which would actually provide an incentive for trans-boundary cybercrime. Nevertheless, it seems that internal cyber-security protocols are a necessary first step towards addressing the problem of trans-boundary harm.

The Russian Government must now first approve the proposal. After approval, a working group comprised of members of the Security Council of the Russian Federation and other federal bodies, as well as representatives from public and private groups working on cyber issues, would be organized to develop specific protocols for the implementation of the plan.[263]

Until such norms are ratified and implemented, Russia will continue to fail in its international obligation to exercise due diligence in the prevention, protection, prosecution and redress of international trans-boundary cybercrime.

Daniel Ortner[264]

Mafia and Its Impact on the Russian Economy, 7 THE MONITOR: J. INT'L STUD. (2000), *available at* http://web.wm.edu/so/monitor/issues/07-1/4-hatcher.htm.

263. Russia has already engaged in laudable public outreach including broadcasting television programs focusing on the new plan. *See* Benjamin Volcsko, *Russia Crowdsourcing It's Cyber Security Strategy: Clever Experiment or Solicitation of Internet Restriction Freedoms?*, MIIS CYSEC (Jan 20, 2014), http://sites.miis.edu/cysec/2014/01/20/russias-crowdsourcing-experiment-getting-the-peoples-opinion-on-the-new-cyber-security-strategy/.

264. Law Clerk for Justice Thomas R. Lee, Utah Supreme Court. I would like to thank Professor Eric Jensen for his tireless assistance on this article.