ADDRESSING GLOBAL CYBERTHREATS THROUGH INTERNATIONAL COLLABORATION

DAVID S. KRAEMER*

The Internet is an increasingly integrated and essential part of everyday life.[1] Many nations employ the Internet in capacities that make it a tool for vital systems and actions, including trade, communication, military, and public utility systems.[2] Any disruption to the Internet can jeopardize the networks responsible for delivery of water, food, fuel, and electricity, placing the lives of those who depend on these systems in jeopardy.[3] While this increased use of the Internet with these systems provides numerous benefits, this dependency places individuals and society at risk should there be a disruption.[4] Cyberattacks[5] pose a major risk to the Internet and have increased in frequency and complexity.[6] Cyberattacks demand an international response as exclusively domestic answers are insufficient for the transnational nature of internet activities and the irrelevance of political borders on the Internet.[7]

For a number of years, cyberattacks were limited in their impact due to the limited number and role of computers. Computer use and integration is increasing dramatically with one billion computers in use

* J.D. 2013, The George Washington University Law School; B.A. 2010, The College of William and Mary.

1. *See* Rex Hughes, *Bits, Bytes and Bullets*, WORLD TODAY, Nov. 2007, at 20–21.

2. *See id.*

3. *See id.* at 22.

4. *See* GA. TECH INFO. SEC. CTR. & GA. TECH RESEARCH INST., EMERGING CYBER THREATS REPORT 2012 2 (2011).

5. A cyberattack is an effort to interrupt or destabilize a computer or computer system. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Human Rights Council, U.N. Doc. A/HRC/17/27 (May 16, 2011) (by Frank Larue) [hereinafter Special Rapporteur]. This includes actions such as entering systems without permission, destroying or altering data within a system, and restricting access to an Internet site by overwhelming the service. *Id.*

6. 18 SYMANTEC CORP., INTERNET SECURITY THREAT REPORT 2013 4 (2013).

7. *See* William Jackson, *Political Borders Don't Stop Cyberattacks, But They Prevent Defense, Study Finds*, G.C.N. (Jan. 30, 2012), http://gcn.com/articles/2012/01/30/cyber-defense-report-political-borders-mcafee.aspx.

in 2008[8] and the next billion expected by 2014.[9] As these computers become integrated in all facets of life, they have become a valuable target. In 2007 and 2008, individuals located in Russia engaged in a large-scale cyberattack against Estonia and Georgia, respectively.[10] These attacks, while not causing much permanent damage, incapacitated the financial, communication, and government functions of these nations.[11] The instances in Russia provide a case study for the potential attacks that cyberattackers could wage against any Internet-reliant nation.[12]

Due to the international scope of this problem, an international response is necessary to regulate the chaotic nature and remedy the increasing number and brazenness of cyberattacks. To achieve this end, the United Nations should expand the mandate of the International Telecommunication Union (ITU) to grant the ITU additional authority over cyberattacks.[13] This new mandate in the form of a treaty would give the ITU a role in the investigation and prosecution of attacks, including analyzing data following an attack, auditing a nation's cybermonitoring systems, and assisting in the development of cybermonitoring systems in those states that lack such a system. This Note is divided into five parts. Part I explains the current design of the Internet and how this structure creates attribution issues. Part II discusses the current sources of threats in the cyberrealm. Part III explores the conflict between individual freedoms and the potential for conflict that exists when trying to regulate the Internet. Part IV analyzes the current and proposed regulations and structures for the Internet. Part V proposes a solution to resolve the issue of cyberattacks by granting new rights and powers to the ITU and placing additional

8. *Computers in Use Pass 1 Billion Mark: Gartner*, REUTERS (June 23, 2008, 8:03 AM), http://www.reuters.com/article/2008/06/23/us-computers-statistics-idUSL2324525420080623.

9. *Number of Personal Computers in Use to Reach 2 Billion by 2014*, PRAVDA.RU, (June 24, 2008), http://english.pravda.ru/science/tech/24-06-2008/105568-computers-0.

10. *Marching off to Cyberwar*, ECONOMIST (Dec. 4, 2008), http://www.economist.com/node/12673385.

11. *Id.*; *Estonia Hit by 'Moscow Cyber War'*, BBC NEWS (May 17, 2007, 3:21 PM), http://news.bbc.co.uk/2/hi/europe/6665145.stm; Travis Wentworth, *You've Got Malice*, DAILY BEAST (Aug. 23, 2008, 8:00 PM), http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html.

12. *See UK Government Warns of Economy's Reliance on Internet*, COMPUTERWEEKLY.COM (Mar. 19, 2008, 4:00 PM), http://www.computerweekly.com/news/2240085424/UK-government-warns-of-economys-reliance-on-internet; *Marching off to Cyberwar*, *supra* note 10.

13. The International Telecommunication Unit (ITU) is a U.N. specialized agency tasked with managing and coordinating telecommunications systems. *History*, ITU, http://www.itu.int/en/about/Pages/history.aspx (last visited Aug. 25, 2013).

requirements on individual states.

I. THE INTERNET

Since 1995, when the National Science Foundation gave up its control over the Internet, the Internet has become increasingly decentralized.[14] Decentralization accords with the basic structure of the Internet, which connects individual networks to one another without central oversight.[15] The network layer[16] connecting the end users[17] together permits anyone to connect without gaining permission.[18] Built with an end-to-end design,[19] the network layer's only role is to transmit the message from source to destination.[20] While the network layer could have been designed to complete a number of different tasks ranging from authenticating data to checking for destructive code, this would have jeopardized the speed, efficiency, and decentralized nature of the network.[21]

This decentralized design can be exploited for malicious actions.[22] Cyberattacks have the potential to cause devastating disruption and damage.[23] Further exacerbating this problem are the innately insecure

---

14. *See* Press Release, TeleGeography, The Global Internet is Decentralizing (Sept. 14, 2011), http://www.telegeography.com/press/press-releases/2011/09/14/the-global-internet-is-decentralizing (last visited Sept. 12, 2013); Pamela Licalzi O'Connell, *Beyond Geography: Mapping Unknowns of Cyberspace*, N.Y. TIMES (Sept. 30, 1999), http://www.nytimes.com/1999/09/30/technology/beyond-geography-mapping-unknowns-of-cyberspace.html.

15. *See* DAVID POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 25 (2009).

16. The network layer is the part of a computer system that is responsible for sending and directing information on the Internet. *See The 7 Layers of the OSI Model*, WEBOPEDIA (June 6, 2013), http://www.webopedia.com/quick_ref/OSI_Layers.asp.

17. An end user is any individual who ultimately uses the respective service, which, in the case of the Internet, refers to the individual who connects to the Internet. *See End User*, TECHOPEDIA, http://www.techopedia.com/definition/610/end-user (last visited Aug. 28, 2013).

18. *See* POST, *supra* note 15, at 80–85.

19. The end-to-end design means that the intelligence of the system lies with the computers on either end of the network, not within the network itself. *See End-to-End Design*, THEFREEDICTIONARY, http://encyclopedia2.thefreedictionary.com/end-to-end+design (last visited Aug. 28, 2013).

20. POST, *supra* note 15, at 80, 83.

21. *Id.* at 84–88.

22. *See* CHAIRMAN OF THE JOINT CHIEFS OF STAFF, DEP'T OF DEFENSE, NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS, D-1 (2006) [hereinafter MILITARY STRATEGY FOR CYBERSPACE], *available at* http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (last visited Aug. 28, 2013)

23. Jeanne Meserve, *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN NEWS (Sept. 26, 2007, 3:06 AM), http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html.

communication procedures and insecure software, and an increasing number of systems that connect to the Internet.[24] Most activity on the Internet is traceable back to its source with the use of one's Internet Protocol (IP) address;[25] but simple methods are available to disguise the IP address and other origin data, thus effectively making the Internet user anonymous.[26]

Ostensibly, masking one's IP address appears to be useful for engaging solely in illegal or other nefarious activities, but there are legitimate justifications.[27] For instance, individuals living under a repressive regime may seek anonymity through masking their IP address to speak against the government.[28] Reporters Without Borders, an organization that advocates for freedom of information, has published the *Handbook for Bloggers and Cyber-Dissidents* which explains not only how to blog, but how to remain anonymous while doing so.[29] This manual assists those attempting to speak out while preventing the government, or anyone else, from positively identifying who published critical or otherwise disallowed text.[30] Nevertheless, while there are legitimate purposes for hiding one's IP address, hackers can utilize these same techniques used for freedom of expression to hide the source of their attack.[31]

This fundamental ability to hide the request's source is one of the chief problems with cyberattacks, since the victim is unable to find the blameworthy party and hold them accountable.[32] Even if the target is prepared, it is difficult to find the exact source of an attack because these cyberattacks often hide their sources through sophisticated means

---

24. *See* MILITARY STRATEGY FOR CYBERSPACE, *supra* note 22, at D-1.

25. *See How to Hide Your IP Address?*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet/basics/hide-ip-address.htm (last visited Aug. 28, 2013). An Internet Protocol (IP) address is a distinctive identifier for a computer on a network. Stephanie Crawford, *What Is an IP Address?*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet/basics/question549.htm (last visited Aug. 28, 2013).

26. *See* Larry Greenemeier, *Seeking Address: Why Cyber Attacks are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), http://www.scientificamerican.com/article.cfm?id=tracking-cyber-hackers.

27. *See* Jonathan D. Glater, *Privacy for People Who Don't Show Their Navels*, N.Y. TIMES (Jan. 25, 2006), http://www.nytimes.com/2006/01/25/technology/techspecial2/25privacy.html.

28. *Id.*

29. REPORTERS WITHOUT BORDERS, HANDBOOK FOR BLOGGERS AND CYBER-DISSIDENTS (Mar. 2008), *available at* http://en.rsf.org/IMG/pdf/guide_gb_md-2.pdf (last visited Sept. 12, 2013).

30. *Id.* at 46–53.

31. *See* Greenemeier, *supra* note 26.

32. *See id.*

beyond simply disguising their IP address.[33] Strictly relying on technical means to determine an attack's source is often insufficient and requires additional investigation to determine the attacker's identity.[34] Further aggravating this problem is the lack of any significant international cooperation, especially as these attacks can quickly cross national borders.[35] International cyberattacks often run through several nations—even using computers in an intermediary state to carry out the attack—and create a significant international dilemma.[36]

II. THREATS IN THE CYBER-REALM

Currently, there are two major sources of cyberattacks: non-state actors and nation states.[37]

A. *Non-State Actors*

Organized cybercriminals and hactivists are the two main types of non-state actors who carry out cyberattacks.[38] While these non-state actors may have different intentions, methods, and objectives, the result on the victim is largely the same.

1. Organized Cybercriminals

Organized cybercriminals act primarily through previously infected computers to carry out attacks on sources such as businesses, individuals, and the military.[39] The cybercriminals often market their tools, access, and techniques to clients for a significant profit.[40] The services provided by some of these organizations parallel legitimate

33. *Id.*

34. *See id.*

35. *See id.*

36. *See id.*

37. *See* Will Rodgers, *Cyber Security, Non-State Threats, and the Electric Grid*, CENTER FOR NEW AM. SECURITY (Feb. 22, 2012, 9:29 AM), http://www.cnas.org/blogs/naturalsecurity/2012/02/cyber-security-non-state-threats-and-electric-grid.html.

38. *See* John Oltsik, *Hacktivism and Cyber Crime Pose the Biggest Threat to Enterprise Organizations*, NETWORK WORLD (Apr. 25, 2012, 4:21 PM), http://www.networkworld.com/community/blog/hacktivism-and-cyber-crime-pose-biggest-threat-enterprise-organizations; *infra* Parts II.A.1–2.

39. *See* FORTINET, CYBERCRIMINALS TODAY MIRROR LEGITIMATE BUSINESS PROCESSES 6 (2013) [hereinafter CYBERCRIMINALS TODAY], *available at* http://www.fortinet.com/sites/default/files/whitepapers/Cybercrime_Report.pdf; Robert Wainwright, *Dealing with Cybercrime – Challenges and Solutions*, GLOBAL ECON. SYMP., http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/dealing-with-cyber-crime-2013-challenges-and-solutions (last visited Aug. 28, 2013).

40. CYBERCRIMINALS TODAY, *supra* note 39, at 3–4, 7.

businesses to the extent that advanced cybercriminals conduct marketing, provide customer support, engage in research and development, and maintain a quality assurance process.[41]

Cybercrime thrives in the absence of strong enforcement.[42] In the power vacuum that followed the collapse of the Soviet Union, former government cyberspies joined organizations such as the Russian Mafia and Russian Business Network, providing these organizations with the expertise necessary to carry out cyberattacks.[43] The former cyberspies used their specialized knowledge, developed in service of the Soviet government, to engage in a number of cyberattacks, including attacking businesses in search of valuable intellectual property.[44]

2. Hacktivists

Hacktivists are the individuals or groups who use the tools of hacking to engage in activism on the web.[45] Unlike organized cybercriminals, the goal of hacktivists is political change, rather than monetary gain.[46] Two well-known groups of hacktivists that have earned publicity recently are Anonymous and LulSec.[47] Most often, the damage inflicted by these groups is concentrated in the cost associated with the remediation for a data breach, brand damage, and downtime.[48] Harm, however, befalls individual consumers as well because the hacktivists steal their private information and may disclose it as part of the organization's hacktivism.[49] Consumers may be further injured when, because of an attack, the services they have paid for and rely upon are no longer accessible. For example, hacktivists have attacked financial services such as PayPal and entertainment services including the Sony

41. *Id.* at 3–6.

42. *See* David Goldman, *The Cyber Mafia Has Already Hacked You*, CNN MONEY (July 27, 2011, 9:45 AM), http://money.cnn.com/2011/07/27/technology/organized_cybercrime/index.htm.

43. *Id.*

44. *Id.*

45. Chris Vallance, *Activists Turn 'Hacktivists' on the Web*, BBC NEWS (Mar. 16, 2010, 10:50 AM), http://news.bbc.co.uk/2/hi/technology/8567934.stm.

46. *See id.*

47. *See* Tim Lohman, *Hacktivism: The Fallout from Anonymous and LulzSec Part 2*, COMPUTERWORLD (Oct. 11, 2011, 7:26 PM), http://www.computerworld.com/s/article/9220759/Hacktivism_The_fallout_from_Anonymous_and_LulzSec_Part_2.

48. Fahmida Y. Rashid, *Targeted Attacks, Hactivism, Mobile Malware Major 2011 Security Trends*, EWEEK (Dec. 27, 2011), http://www.eweek.com/c/a/Security/Targeted-Attacks-Hacktivists-and-Malware-Major-Trends-in-Security-in-2011-530955.

49. *See* Byron Acohido, *Power, Glory Fuel Hacktivism Against Companies*, USA TODAY (June 13, 2011, 8:33 AM), http://www.usatoday.com/tech/news/2011-06-11-hacktivists_n.htm.

PlayStation Network.[50] While hacking can cause significant damage, two hacktivist actions greatly exceed the previous examples: the patriotic Russian attacks on Estonia and Georgia.

a. 2007 Cyberattacks on Estonia

In Estonia, cyberattacks employed by patriotic Russian hacktivists led to the disruption of all Internet services of Estonia, one of the most wired countries in the world.[51] Estonia is especially susceptible to cyberattacks as the government, banks, elections, and most services rely on the Internet.[52] In 2007, the Estonian government was debating the removal of a bronze statue built by the Soviet Union in Estonia's capital.[53] Moscow objected strongly, arguing that removal of the statue would denigrate World War II-era Soviet soldiers.[54] The Estonian people increasingly objected to the statue's presence because they viewed it as a memorial to the occupation of the Baltic countries by the Soviets.[55] This conflict culminated in "Bronze Night," the April 27, 2007, riot when the Estonian military removed the statue to a new site away from the unrest.[56] The Russian media and government objection helped lead to a strong patriotic response among the Russian population.[57]

In the days and weeks following the removal of the statue, state-run and private websites in Estonia were hit with a Distributed Denial of Service (DDoS)[58] attack.[59] The DDoS attack relied on thousands of computers, previously infected unbeknownst to their owners, which sat idly by waiting for an order.[60] Upon receiving an order, the infected computers participated in the largest cyberattack to date, first taking out publicly known websites,[61] then advancing to sites unknown to the

50. *Id.*

51. *See* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

52. *Estonia Hit by 'Moscow Cyber War'*, *supra* note 11.

53. *See* Davis, *supra* note 51.

54. RICHARD A. CLARKE & ROBERT A. KNAKE, CYBER WAR 13 (2010).

55. *See id.* at 12–13.

56. *Id.* at 13.

57. *Id.*

58. A Distributed Denial of Service (DDoS) attack is a type of cyberattack in which the goal is to make a website or other service unavailable by overwhelming the system with a significant number of requests. *Id.* at 13–14. DDoS attacks are carried out by networks of infected computers all requesting information from one website or service at the same time, thus tying up the target's system and causing it to fail. *Id.*

59. *Id.* at 13; *Estonia Hit by 'Moscow Cyber War'*, *supra* note 11.

60. *See* CLARKE & KNAKE, *supra* note 54, at 14.

61. *Id.* at 14–15; *Estonia Hit by 'Moscow Cyber War'*, *supra* note 11.

public—including the servers responsible for telephones, credit cards, and the Internet directory—effectively knocking these services offline and disrupting the ability to conduct commerce and communicate.[62]

While undergoing the attack, the Estonian defense ministry attempted to track the attacks, noting that they came from all corners of the globe.[63] Estonia utilized the assistance of both the North Atlantic Treaty Organization (NATO) and the European Union to attempt to ascertain who was responsible for the attack.[64] Utilizing a back-tracing technique, the agencies tried to determine the source by monitoring communications from the attacking computers.[65] Tracking became more difficult as Russia refused to cooperate with the investigation, violating a bilateral agreement requiring cooperation.[66]

Eventually, many of the final source computers were located in Russia.[67] The fact that the hackers used a code written on a Cyrillic-alphabet keyboard supported the assumption that the attack originated from Russia.[68] Andrus Ansip, the Estonian Prime Minister, placed the blame at the feet of Moscow.[69] Russia continually asserted that the cyberattacks against Estonia were from patriotic Russians conducted on their own.[70] Nevertheless, Russia did not seek to prosecute the vigilantes allegedly responsible for this attack.[71] If the Russian story is true, it is a prime example of the impact of hacktivists. Even if Moscow did have a hand in the attack, this cyberattack against Estonia demonstrates how a state can avoid liability by not cooperating.

b. 2008 Cyberattacks on Georgia

Whereas the attacks on Estonia targeted the economy and communications systems, the cyberattack waged on Georgia during the South Ossetia War coincided with a conventional military attack from Russia.[72] Following missile strikes on Georgia from South Ossetia and Georgia's subsequent missile response, Georgia invaded and then was expelled from South Ossetia by the Russian army.[73] At the same time

62. CLARKE & KNAKE, *supra* note 54, at 15.
63. *Estonia Hit by 'Moscow Cyber War'*, *supra* note 11.
64. *Id.*
65. CLARKE & KNAKE, *supra* note 54, at 15.
66. *Id.*
67. *See id.*
68. *See id.*
69. *Estonia Hit by 'Moscow Cyber War'*, *supra* note 11.
70. CLARKE & KNAKE, *supra* note 54, at 15–16.
71. *Id.* at 16.
72. *Id.* at 18.
73. *Id.*

as the Russian attack, individuals in Russia launched cyberattacks, with evidence suggesting their preparation began over two weeks before the first missile strikes.[74] The cyberattack initially launched requests at the Georgian websites in a DDoS attack, resulting in the shutdown of numerous servers for the government, media, and banks.[75] In addition to taking down the Georgian websites, the inbound traffic was so heavy that outbound traffic from Georgia was no longer possible, severing Georgian communications with the rest of the world.[76] The DDoS attack not only prevented dissemination of news, but also shut down all access to Georgian credit cards and mobile phones.[77]

Similar to the assertion following the 2007 cyberattack on Estonia, Russia claimed that Russian citizens, spurred on by patriotic vehemence, were responsible for the cyberattacks against Georgia in 2008.[78] Based on further investigation, it appears that the hackers needed both advanced knowledge of the Russian attack and close cooperation with Moscow to enable the cyberattacks and military actions to occur in sync to support Russia's military objectives in the 2008 South Ossetia War.[79] If the Russian story is truthful, it furnishes another instance of the strength of hacktivism. Nonetheless, the use of cyberattacks in both Georgia and Estonia by Russian patriotic hackers and the subsequent Russian refusal to assist demonstrate the attribution problem that plagues attacks from cyberspace and how international cooperation is vital in combating cyberattacks.

B. *Nation-States*

The final source of cyberattacks is nation-states, who view the Internet as both a vital tool and a new battlefield.[80] Individual governments are capable of developing and employing the most sophisticated and effective cyberweapons because they have vast economic resources.[81] By recent estimates, governments spend nearly

74. John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

75. Wentworth, *supra* note 11.

76. CLARKE & KNAKE, *supra* note 54, at 19.

77. *Id.* at 20.

78. *Id.*

79. *See* Mark Rutherford, *Report: Russian Mob Aided Cyberattacks on Georgia*, CNET (Aug. 18, 2009, 8:53 PM), http://news.cnet.com/8301-13639_3-10312708-42.html.

80. *See* CLARKE & KNAKE, *supra* note 54, at 27–30 (describing North Korea's use of cyberattacks).

81. *See* Press Release, Visiongain, 'The Cyberwarfare Market Worth $15.9bn in 2012' Says Visiongain Report (Dec. 6, 2011), http://www.visiongain.com/Press_Release/114/'The-cyberwarfare-market-worth-15-9bn-in-2012'-says-visiongain-report (noting size of government

$16 billion per year on offensive and defensive capabilities for cyberwarfare.[82]

Cyberwarfare allows traditionally weak nations to employ readily available tools on the Internet or employ a limited number of cyberwarriors to cause substantial damage.[83] Weak states, which otherwise are outspent on kinetic weaponry, can now wreak significant damage on other nations without large expenditures.[84]

China's emergence as a powerhouse in the area of cyberattacks is a source of significant concern.[85] Attacks originating from China have targeted a number of victims, including the U.S. Chamber of Commerce, the United Nations, the International Olympic Committee, and many other businesses and governmental organizations.[86] While China has publicly denied that they engage in cyberattacks, they inadvertently disclosed one cyberweapon on national television during the "The Cyber Storm Has Arrived!" documentary.[87] Aired on China Central Television, a six-second clip in the documentary showed a hacking tool that could launch a DDoS attack against websites in other countries.[88] One specific website listed in the program was a Falun Gong website hosted at the University of Alabama at Birmingham.[89]

This is not the first time that China targeted political activists. In 2010, Google revealed that cyberattacks originating in China targeted the Gmail accounts of Chinese human rights activists.[90] Although the

---

spending on cyberwarfare).

82. *Id.* Cyberwarfare is an act by a nation against the networks or computers of another nation with the intent to hamper, disturb, or destroy said systems to achieve national, strategic, or military objectives. CLARKE & KNAKE, *supra* note 54, at 6.

83. Jeffrey Barlow, *Cyber War and U.S. Policy: Part I, Neo-Realism*, J. EDUC. COMMUNITY & VALUES (June 2010), http://bcis.pacificu.edu/journal/article.php?id=682.

84. *Id.*

85. *See* FREEDOM HOUSE, FREEDOM ON THE NET 2011 5 (Sanja Kelly & Sarah Cook, eds., 2011).

86. Michael Riley, *Hackers in China Breach Olympic, UN Networks, Security Firms Say*, BLOOMBERG BUSINESSWEEK (Aug. 4, 2011), http://www.businessweek.com/news/2011-08-04/hackers-in-china-breach-olympic-un-networks-security-firms-say.html; Siobhan Gorman, *China Hackers Hit U.S. Chamber*, WALL ST. J. (Dec. 21, 2011), http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html.

87. Ellen Nakhima & William Wan, *China's Denials About Cyberattacks Undermined by Video Clip*, WASH. POST (Aug. 24, 2011), http://www.washingtonpost.com/world/national-security/state-media-video-candidly-depicts-chinas-developing-cyber-weaponry/2011/08/22/gIQAqyWkbJ_story.html.

88. *Id.*; Robert McMillan & Michael Kan, *China Hacking Video Shows Glimpse of Falun Gong Attack Tool*, COMPUTERWORLD (Aug. 23, 2011, 6:43 PM), http://news.idg.no/cw/art.cfm?id=AFFF529D-1A64-6A71-CE8EB40568F95140.

89. *Id.*

90. Kim Zetter, *Google to Stop Censoring Search Results in China After Hack Attack*, WIRED (Jan. 12, 2010, 7:10 PM), http://www.wired.com/threatlevel/2010/01/google-censorship-

United States did not accuse the government of China directly of the attack, a U.S. diplomatic channel leaked evidence to support the belief that the Chinese Politburo was directly responsible.[91]

Attacks originating from China are targeting government and commercial computers for espionage.[92] One example of Chinese attacks is the computer virus targeted at the U.S. unmanned drone fleet.[93] This virus, called Sykipot, looked for information on two highly advanced drones: the Boeing X-45 and X-37B.[94] The X-37B, an unmanned orbital vehicle, executed a classified mission in 2011 to test the vehicle[95] and would undoubtedly be a high-value target for Chinese espionage. The virus also targeted smart-card credentials used by the U.S. Department of Defense.[96] These smart-card credentials are part of a multi-step authentication that requires both the username and password, as well as access to a physical device that displays a changing passcode to login.[97] Through access to the Department of Defense's code, the hackers effectively remove one security layer for accessing the systems of the Defense Department.[98]

C. *Increasing Threat*

Both sources of cyberattacks are going to become increasingly dangerous in the coming years.[99] Not only are nation-states spending more for their own cyberweaponry and defense, but also organized

---

china.

91. Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES (Nov. 29, 2010), http://www.nytimes.com/2010/11/29/world/29cables.html.

92. U.S. – CHINA ECON. & SEC. REVIEW COMM'N, 2008 REPORT TO CONGRESS 165 (Nov. 2008).

93. Robert Johnson, *New Evidence Suggests China's Hacking into US Drones Using Adobe Reader and Internet Explorer*, BUSINESS INSIDER (Dec. 22, 2011, 8:51 AM), http://articles.businessinsider.com/2011-12-22/news/30545577_1_virus-pdf-files-adobe-reader.

94. *Id.*

95. Robert Johnson, *The X-37B Mystery Spacecraft Just Had Its Nine Month Mission Extended Indefinitely*, BUSINESS INSIDER (Dec. 3, 2011, 9:15 AM) http://www.businessinsider.com/the-x-37b-air-force-mystery-spacecraft-just-had-its-nine-month-mission-extended-2011-12.

96. Kelly Jackson Higgins, *Sykipot Malware Now Steals Smart-Card Credentials*, DARK READING (Jan. 12, 2012), http://www.darkreading.com/authentication/167901072/security/attacks-breaches/232400288/sykipot-malware-now-steals-smart-card-credentials.html.

97. *Understanding and Implementing Smart Card Authentication*, TECH-FAQ, http://www.tech-faq.com/understanding-and-implementing-smart-card-authentication.html (last visited Aug. 29, 2013).

98. *See* Higgins, *supra* note 96.

99. *See* Lieu Thi Pham, *Cyber Crime Ramps up in 2012*, SMARTPLANET (Jan. 13, 2012, 4:15 AM), http://www.smartplanet.com/blog/global-observer/cyber-crime-ramps-up-in-2012/2627.

cybercriminals are advancing more sophisticated tools to take advantage of computer systems.[100] Hacktivists, meanwhile, become more developed and knowledgeable in conducting their activism.[101]

III. THE CONFLICT BETWEEN WAR AND PRIVACY

Cyberattacks raise significant concerns in the military realm as well as among those advocating for individual freedoms on the Internet. These concerns represent a dichotomy of views that are prevalent in the debate regarding the regulation of the Internet.

A. *Cyberattacks as a Rationale for Kinetic War*

For a long time, experts believed that cyberattacks could not extend their damage beyond affecting computers and their systems.[102] A test conducted by the U.S. Department of Homeland Security in which a cyberattack caused a generator to seriously malfunction, shattered this perception.[103] The test, code named Aurora, demonstrated that, beyond deactivating elements essential to the electrical grid, cyberattacks could cause significant damage to vital machinery.[104] This kind of attack, if launched on a scale large enough to disrupt power to one-third of the United States for three months, could cost $700 billion.[105]

Homeland Security Secretary Janet Napolitano has said that cyberattacks have nearly shut down critical services in the United States, including financial services and transportation systems.[106] Napolitano also asserted that attacks on the national infrastructure could result in deaths.[107] Shawn Henry, the Executive Assistant Director of the Federal Bureau of Investigation, reiterated this assertion.[108]

Real-world attacks on industrial equipment have also occurred with the malware worm known as Stuxnet.[109] Stuxnet is a type of software that specifically targeted Siemens supervisory control and data

100. *Id.*
101. *Id.*
102. *See* Meserve, *supra* note 23.
103. *Id.*
104. *Id.*
105. *Id.*
106. Fahmida Y. Rashid, *Cyber-Attackers Already Targeting Critical Infrastructure: DHS*, EWEEK (Oct. 30, 2011), http://www.eweek.com/c/a/Security/CyberAttackers-Already-Targeting-Critical-Infrastructure-DHS-573564.
107. *Id.*
108. *Id.*
109. *Software Smart Bomb Fired at Iranian Nuclear Plant: Experts*, ECON. TIMES (Sept. 24, 2010, 7:46 AM), http://articles.economictimes.indiatimes.com/2010-09-24/news/27613333_1_ralph-langner-stuxnet-software-security-researchers.

acquisition systems used by the Iranian nuclear program.[110] Stuxnet first searched for the specific Siemens machines with motors moving at 1064 revolutions per second: the speed required for uranium centrifuges that is also in the configuration found at the Iranian nuclear centrifuge facility in Natanz.[111] When Stuxnet found this precise setup, it would take over control of the system, altering the revolution speed by speeding the motors to 1410 revolutions per second, damaging the centrifuge, and then slowing down the motors to two revolutions per second, effectively reversing the enrichment process by having the various isotopes mix again.[112] Carrying out this precise pattern repeatedly, Stuxnet would simultaneously suppress any alerts to the control machines about any malfunctions, effectively masking its effects.[113]

This worm's apparent purpose demonstrates the effective employment of a cyberattack on an industrial system in the real world.[114] Although cyberattacks to date have been comparatively limited in their scope, the potential for "an 'ePearl Harbour' or an 'e-911'" is an ever-present concern that could reduce a first world nation to a third.[115] The potential devastation creates an imperative endeavor among all developed nations to protect the vital systems to stay a catastrophic attack.[116]

B. *Expansion of the Realms of Warfare*

Warfare traditionally consisted of four realms: land, sea, air, and space.[117] Given the increasing domestic dependence on the Internet and the potential for cyberattacks to shift the tide of war, the United States has stepped up its cyberwarfare capabilities.[118] While an attack through cyberspace could devastate domestic functions, the U.S. military also relies on cyberspace operations to ensure its technical war fighting ability.[119] The United States has set a goal of establishing superiority

110. *See id.*

111. *Stuxnet the World's Dirtiest Digital Bomb*, ABC SCIENCE (Nov. 1, 2011), http://www.abc.net.au/science/articles/2011/11/01/3353334.htm.

112. *Id.*

113. *See Software Smart Bomb Fired at Iranian Nuclear Plant: Experts*, *supra* note 109.

114. *See Stuxnet the World's Dirtiest Digital Bomb*, *supra* note 111.

115. Hughes, *supra* note 1, at 20.

116. *See generally id.* at 20–22 (encouraging the international community to take more precautions and establish an international legal framework to guard against cyber attacks).

117. *See War in the Fifth Domain*, ECONOMIST (July, 1, 2010), http://www.economist.com/node/16478792.

118. *Id.*

119. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, *supra* note 22, at 9.

over this manmade realm through a number of means, most notably kinetic actions.[120]

The United States is not alone in seeking such supremacy, and there are concerns that a contest for supremacy could provoke a cyberarms race.[121] To date, this conflict has largely been limited to espionage and conflicts paralleling the Cold War proxy wars between the United States and the Soviet Union (USSR) and thus has been titled a "Cyber Cold War."[122] As nuclear weapons were the key strategic weapon of the Cold War, cyberweapons could create similar devastation and are increasing in a manner similar to a nuclear arms race as nations seek to match their perceived opponents.[123] Not all nations have similar information infrastructures; thus, mutually assured destruction in the cyberrealm is not always possible.[124] Because a cyberattack would likely be ineffective against a technically inferior nation, the United States may employ kinetic forces as a tool for retribution to a cyberattack, thus preserving a philosophy similar to mutually assured destruction theory.[125] The potential for a cyberattack leading to war creates a strong case for a restriction of the Internet. The opposing viewpoint, however, sees the restriction of the Internet as not only an affront to individual rights, but also as crippling the elements that made the Internet so important, as the following Section discusses.[126]

C. *The Importance of Internet Freedom and Access*

Part of what makes the Internet such an effective tool is its openness.[127] This characteristic helps encourage not only innovation,

120. *See id.* at ix.

121. David Goldman, *China vs. U.S.: The Cyber Cold War is Raging*, CNN MONEY (July 28, 2011, 8:43 AM), http://money.cnn.com/2011/07/28/technology/government_hackers/index.htm (comparing the cybersecurity activities of the United States and China to the Cold War).

122. Michael Riley & John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG BUSINESSWEEK (Dec. 22, 2011), http://www.businessweek.com/news/2011-12-22/china-based-hacking-of-760-companies-shows-cyber-cold-war.html.

123. Gautham Nagesh, *Retired Air Force Lt. Gen. Says US in 'Cyber Cold War'*, THE HILL (Sept. 23, 2011, 11:22 AM), http://thehill.com/blogs/hillicon-valley/technology/183565-retired-air-force-lt-gen-says-us-in-cyber-cold-war.

124. *See id.* (describing the idea that the United States should be prepared to respond to a cyberattack with more traditional forms of military retaliation).

125. *See id.*

126. Maureen Cosgrove, *UN Warns Internet Restrictions Violate Human Rights*, JURIST (June 3, 2011, 3:16, PM), http://jurist.org/paperchase/2011/06/un-warns-internet-restrictions-violate-human-rights.php.

127. *In Praise of Chaos*, ECONOMIST (Oct. 1, 2011), http://www.economist.com/node/21531011.

but also freedom due to lack of censorship.[128] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression declared, "Given that the internet has become an indispensable tool for realizing a range of human rights, . . . ensuring universal access to the Internet should be a priority for all States."[129] The actions of individual nations, including Finland and Estonia, in making Internet access a human right within their borders bolsters the viewpoint of Internet access as a fundamental right.[130] A U.N. Special Rapporteur has emphasized that any limitation of the right of freedom of expression on the Internet must meet all aspects of a general three-part test:

> (a) It must be provided by law, which is clear and accessible to everyone . . . and (b) It must pursue one of the [following] purposes . . . (i) to protect the rights or reputations of others, or (ii) to protect national security or of [sic] public order, or of [sic] public health or morals . . . and (c) It must be proven as necessary and the least restrictive means required to achieve the purported aim.[131]

Cyberattacks often constitute restrictions of freedom of expression.[132] For example, a DDoS attack, which causes certain web sites or systems to crash, prevents the dissemination of the information.[133] States have a positive requirement to protect an individual's right to freedom of expression by protecting the individual from interference by third parties.[134] The obligations include investigating the attack, holding those responsible liable, and preventing such attacks from happening again.[135] Thus, there is a tension between defending from cyberattacks and preserving the freedom of expression on the Internet.

IV. CURRENT AND PROPOSED REGULATION STATUS AND STRUCTURES

As it stands today, the Internet has neither central control nor formal structural organization.[136] While this design encourages innovation and free speech, states are concerned with such an unrestrained system.[137] Thus far, legislation has been limited to regional and individual states,

---

128. *See id.*

129. Special Rapporteur, *supra* note 5, at 22.

130. *See Internet Access is 'a Fundamental Right'*, BBC NEWS (Mar. 8, 2010, 8:52 AM), http://news.bbc.co.uk/2/hi/8548190.stm.

131. Special Rapporteur, *supra* note 5, at 8.

132. *Id.* at 14–15.

133. *Id.*

134. *Id.* at 15.

135. *Id.*

136. *See In Praise of Chaos*, *supra* note 127.

137. *Id.*

yet a solution that looks at the problem on an individual state or regional level is inadequate because this global problem necessitates a global solution.[138]

A. *Regional Legislation*

Created by the Council of Europe, the International Convention on Cybercrime, also known as the Budapest Convention, was the first of its kind.[139] The Budapest Convention came into effect on July 1, 2004, and covers a number of offenses.[140] These include "illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, . . . [and] offenses related to copyright and neighbouring rights."[141] The Convention establishes permitted national actions, specifically for the assembly and retention of data for a criminal case.[142] This includes "expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; and interception of content data."[143] Finally, the treaty includes provisions for extradition and mutual assistance between the states.[144] As of November 28, 2010, thirty states have signed and ratified the treaty, with only one non-member state of the Council of Europe, the United States, ratifying the treaty.[145]

While this convention appears to cover many areas, there are significant shortfalls. First, and most obviously, it is essentially restricted to Europe and limits the ability for new states to participate.[146] To join, unanimous consent of the member states is required, thus

---

138. *See* Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Braz., Apr. 12–19, 2010, *Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime*, para. 31, U.N. Doc A/CONF.213/9 (Jan. 22, 2010) [hereinafter U.N. Crime Prevention and Criminal Justice].

139. *See* UNESCO, THE COE INTERNATIONAL CONVENTION ON CYBERCRIME BEFORE ITS ENTRY INTO FORCE 1 (Jan.–Mar. 2004), *available at* http://portal.unesco.org/culture/en/files/19556/11515912361coe_e.pdf/coe_e.pdf.

140. *Id.*

141. *Id.*

142. *Id.* at 2.

143. *Id.*

144. Convention on Cybercrime arts. 24–25, Nov. 23, 2001, T.I.A.S. No. 13174, E.T.S. No. 185.

145. *Status of Convention on Cybercrime as of 28/10/2010*, COUNCIL EUR., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG (last visited Sept. 3, 2013).

146. *See id.*, U.N. Crime Prevention and Criminal Justice, *supra* note 138, para. 34.

establishing a strong barrier to entry.[147] As a further inhibitor of increased membership, states considering joining have to take the treaty as is without the ability to negotiate.[148]

There are additional issues with the Convention on Cybercrime itself that make this treaty insufficient.[149] First, Hamadoun Touré, Secretary General of the ITU, has spoken against the usage of the Convention on Cybercrime as a standard.[150] Some have suggested that the treaty is not suitable for a global role due to its development for European concerns and outdated rules.[151] Concerns exist regarding the use of the treaty to force states to administer the cyberlaws from other countries, even if a user's actions are legal in the host nation.[152] This could include obligations to restrict free speech, such as requiring investigative agencies to monitor individuals or to force Internet service providers to log users' activities without due process.[153]

In 2003, the Convention on Cybercrime added an Additional Protocol requiring the criminalization of the distribution of racist or xenophobic material on the Internet.[154] Thirty-one nations signed onto this new protocol, but only six states ratified the new portion.[155] The Additional Protocol adds an undoubtedly European focus as the Explanatory Report of the Additional Protocol specifically references Holocaust denial and gross minimization as part of the rationale for the need for the additional protocol.[156] This European partiality buttresses the complaints leveraged by Touré against the utilization of the Convention on Cybercrime as a global standard.

B. *Proposals for Global Agreements*

Other proposals for possible global agreements exist, one of which is

147. *Id.*

148. *See id.* para. 35.

149. *See* Brian Harley, *A Global Convention on Cybercrime?*, COLUM. SCI. & TECH. L. REV. (Mar. 23, 2010), http://www.stlr.org/2010/03/a-global-convention-on-cybercrime.

150. *Id.*

151. *Id.*

152. Nate Anderson, *"World's Worst Internet Law" Ratified by Senate*, ARS TECHNICA (Aug. 4, 2006, 12:57 PM), http://arstechnica.com/old/content/2006/08/7421.ars.

153. *Id.*

154. Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems art. 3.1, Jan. 28, 2003, E.T.S. No. 189 [hereinafter Additional Protocol].

155. *Status of Additional Protocol to the Convention on Cybercrime*, COUNCIL EUR., http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=17/02/2006&CL=ENG (last visited Sept. 3, 2013).

156. Additional Protocol, *supra* note 154, Explanatory Report paras. 39–40.

the International Code of Conduct for Information Security.[157] When filing this proposal, China, Russia, Tajikistan, and Uzbekistan called for a discussion regarding establishing standards.[158] The proposal itself contained a set of principles implementable in both the military and civilian spheres.[159] This agreement creates a general standard that could potentially afford permission to a state to block a communication for any number of reasons.[160] The agreement's authority could lead to limitations on international communications and enable states to ask other signatories to start blocking access to information on topics sensitive to them, such as the Falun Gong for China.[161] Another option is to expand the ITU's mandate to give it more authority in the realm of cyberattacks including investigating, prosecuting, and aiding in development of monitoring systems, which will be discussed below.

C. *Current Status of the International Telecommunication Union*

The ITU is an organization with a long history of involvement with all forms of telecommunications.[162] Originally founded in 1865 as the International Telegraph Union, its role evolved to include coordinating and managing wired and wireless communications, necessitating the change of its name to the International Telecommunication Union.[163] The ITU moved under the auspices of the United Nations with an agreement in 1947 that made the ITU a U.N. specialized agency.[164] In 1989, the ITU's role expanded to include technically assisting developing countries with their communication technologies.[165] Given the haphazard development of the ITU, the Additional Plenipotentiary Conference remodeled the ITU in 1992, establishing three main sections: Telecommunication Standardization (ITU-T), Radiocommunication (ITU-R), and Telecommunication Development (ITU-D).[166] As of September 2013, there are 193 nations and in excess

157. *China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations*, MINISTRY FOREIGN AFF. CHINA (Sept. 13, 2011), http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm.

158. *Id.*

159. *Id.*

160. Nate Anderson, *Russia, China, Tajikistan Propose UN "Code of Conduct" for the 'Net*, ARS TECHNICA (Sept. 20, 2011, 1:53 PM), http://arstechnica.com/tech-policy/news/2011/09/russia-china-tajikistan-propose-un-code-of-conduct-for-the-net.ars.

161. *Id.*

162. *See Overview of ITU's History*, INT'L TELECOMM. UNION, http://www.itu.int/en/history/Pages/ITUsHistory.aspx (last visited Sept. 3, 2013).

163. *Id.*

164. *Id.*

165. *Id.*

166. *See id.*

of 700 non-state entities who are members of the ITU.[167] The world's newest state, the Republic of South Sudan, joined in July 2011.[168]

The ITU's role includes creating a "culture of cyber-security."[169] To do so, the ITU seeks to "build confidence and security in the use of Information and Communication Technologies."[170] This charge, originating from a combination of decisions made at the World Summit on the Information Society, the 2010 ITU Plenipotentiary Conference, and a number of ITU resolutions, creates a significant role for the ITU with cybersecurity efforts.[171] The ITU also supports the prospect of different entities working together to derive the source of an attack, but does not directly require any such action.[172] The reliance on creating a culture of cybersecurity provides a weak foundation for the ITU to achieve major results as it exists today.

V. PROPOSED SOLUTION

A. *Addressing the Problem: Altering the ITU and the States' Responsibilities*

To address the problem of cyberattacks, an international response is necessary due to the international nature of cyberattacks.[173] Two areas of changes are required to reduce the increasing problem of cyberattacks: alterations to the ITU and to state responsibilities. To enable this change, the proposed solution will be in the form of a treaty as an additional optional protocol to the ITU. Included in the treaty will be a provision that requires that a state, if it fails to meet the legal requirements, is liable to the victim state for the attacks in front of the International Court of Justice. The changes will provide an opportunity to develop a successful and less invasive tool for addressing the ever-increasing problem of cyberattacks.

---

167. *Membership*, INT'L TELECOMM. UNION, http://www.itu.int/en/about/Pages/membership.aspx (last visited Mar. 25, 2012).

168. *New Country, New Number*, INT'L TELECOMM. UNION (July 14, 2011), http://www.itu.int/net/pressoffice/press_releases/2011/25.aspx.

169. World Summit on the Information Society, Dec. 10–12, 2003, *Declaration of Principles*, para. 35, WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003); *ITU Activities Related to Cyber Security*, INT'L TELECOMM. UNION, http://www.itu.int/cybersecurity/ (last visited Aug. 29, 2013).

170. *ITU Activities Related to Cyber Security*, *supra* note 169.

171. *Id.*

172. *See* World Telecomm. Standardization Assembly Res. 08 – 50, at 2 (Oct. 21–30, 2008), *available at* http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf.

173. *See* ITU GLOBAL CYBERSECURITY AGENDA & HIGH-LEVEL EXPERTS GROUP, GLOBAL STRATEGIC REPORT 113 (2008).

1. Necessary Changes to the International Telecommunication Union

To achieve a meaningful result for global cybersecurity, a paradigm shift of the ITU's powers needs to occur. This change is a two-fold alteration in the ITU: adding a sector to the organization and expanding the organization's mandate. A new sector for Cybercommunication, abbreviated to ITU-C, will be added to the Radiocommunication, Telecommunication Standardization, and Telecommunication Development sectors that exist currently.[174] The new ITU-C sector would leverage many of the best practices learned through the long history of the ITU. The ITU-C would consist of four distinct groups: (1) an inspection/data analysis group, (2) a development assistance group, (3) an audit group, and (4) a request review board. As the ITU-D developed best practices for state assistance, the ITU-C's development assistance group could leverage this experience and would gain significantly through relations between the ITU-C and ITU-D. The design of the ITU-C's internal structure takes into account the changes necessary for the unique new role afforded to the ITU.

As it stands now, the ITU's primary role of creating a culture of cybersecurity is insufficient; the ITU needs to be able to have a more significant impact. The ITU cybersecurity mandate should shift from one primarily tasked with bringing attention to cyber concerns to a multifaceted, active mission supporting the investigation and prosecution of attacks. The new roles will include analyzing data following an attack, auditing a country's cybermonitoring and defenses, and, should a nation's cyberdefenses fail to reach an acceptable level, assisting individual states in developing such cybermonitoring defenses.

The ability to scrutinize data following an attack is essential for two reasons. First, this ensures that a nation has complied with an investigation request in good faith and certifies that the requests from foreign nations do not exceed permissible limits. The auditing functionality will strengthen the ability of the ITU to hold states responsible for meeting their requirements and accountable for their actions. By enabling the ITU to audit a state's monitoring systems, the ITU can determine if the minimum functionality requirements are in place to ensure that the system can meet all the functional requirements for tracking and ensure that states are not using a system installed by the ITU for impermissible purposes. Although states may initially perceive external audits as a significant concession, for most states that have developed their own systems, the audits would be limited to monitoring

174. *ITU Organizational Chart*, INT'L TELECOMM. UNION, http://www.itu.int/aboutitu/structure/ (last visited Aug. 29, 2013).

the functionality. States may accomplish their monitoring by completing a false cyberattack test and analyzing if the results were within permissible levels.

If a state utilizes the ITU framework and resources to develop their monitoring system, the ITU can gain additional access to the national systems to ensure that the state does not exceed the allowable parameters set forth by the ITU. This is important as states may lack the expertise or the funds necessary to have their own cybermonitoring service to meet the higher standards placed upon them. Thus, the ITU can assist the state to meet the new requirements utilizing a framework and expertise partially developed by the ITU-D in their role of assisting in the development of information technologies.[175] The benefit granted to the state that accepts the new tool will offset any compromise that the state is required to make. In addition to the additional role of the ITU, a modernization of state responsibility for cyberattacks needs to occur.

2. State Responsibility Changes

Under the Bush Doctrine, states are responsible for the actions of individuals within their borders, with Bush specifically asserting, "[w]e will make no distinction between the terrorists . . . and those who harbor them."[176] To escape the liability that would come from having the attacks originate from within their borders, the states should have a two-step process. First, individual states must assist in tracking an attack that either originates or passes through its territory, as failing to assist is perceivable as harboring the hackers. This would entail maintaining basic information, such as logs and tracing reports, and retaining the evidence to ensure later forensic analysis is possible. The exact specifications of such basic, necessary information should be under the discretion of the ITU-C and would be alterable to ensure sufficiency with the evolving state of the Internet. To ensure that a state could provide the requisite information, the state should need to meet a minimum standard developed by the ITU-C to enable attribution for the attack.

Second, if the state determines that the attack came from within its borders and can ascertain the attacker, the state is subject to a mutual prosecution agreement that requires either extradition or prosecution to escape liability. The state, however, would not be liable for the actions

175. *See Welcome to the ITU-D Website*, INT'L TELECOMM. UNION, http://www.itu.int/ITU-D/information/aboutbdt.html (last visited Aug. 29, 2013).

176. *See* George W. Bush, President of the U.S., Statement by the President in His Address to the Nation (Sept. 11, 2001), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/print/20010911-16.html.

of the responsible party where the responsible party is not chargeable with a crime, for instance, if deceased or unascertainable after a good faith effort. Extradition would be most critical in cases where there could be a conflict of interest, such as if the acts of the hacker were carried out to benefit the state itself or a domestic company. Nonetheless, because there are states that refuse extradition of their citizens in any circumstances,[177] a multilateral prosecution agreement is essential to cases where extradition would be inappropriate or refused. This ensures that individuals are unable to escape prosecution simply because they are located in another nation that refuses to extradite. To ensure that certain states do not indirectly promote attacks to originate from within their borders, a requirement of minimum punishments based on the offense is important. This ensures that convictions will carry at least some significance and lessens potential bias that may come from cyberattacks that favor the home state.

The state responsibility assertion for the action of individuals within their states is applicable in a number of the previous examples. For instance, the cyberattacks originating from Russia against Estonia in 2007 and Georgia in 2008 may be attributable to the Russian state. In those circumstances, Georgia and Estonia may have a claim against Russia for harboring the cyberattackers, since the Russians did not do anything to stop these attacks[178] and may have supported them.[179] This understanding is also applicable in the case of Chinese hackers who, like their Russian counterparts, have faced no prosecution or are actively supported by the Chinese government.[180] As such, by holding the state responsible for the actions of their domestic hackers on international targets, this proposal would deter states from harboring or sponsoring the hackers.

3. Procedure for Requesting Assistance

Under the proposed solution, a state that is the target of a cyberattack would report the attack to the ITU-C and provide all relevant information they have. The ITU-C would first review the request to ensure that it was appropriate. Next, the ITU-C would issue requests to other states to preserve relevant data and begin an investigation. Upon

177. *See* Extradition Law of the People's Republic of China (order of the President No. 42), Dec. 28, 2000 (China), *available at* http://www.gov.cn/english/laws/2005-09/22/content_68710.htm.

178. CLARKE & KNAKE, *supra* note 54, at 15, 20.

179. Rutherford, *supra* note 79.

180. Charles Arthur, *Chinese Cyber-Attacks 'Pinned to Users',* GUARDIAN (Dec. 12, 2011, 2:38 AM), http://www.guardian.co.uk/technology/2011/dec/12/china-us-hacking-tensions.

the completion of the investigations, the ITU-C will receive all the information and assist the victim state with the analysis. When the perpetrator is identified, the ITU-C will notify the state where the individual is suspected with any information relevant for the capture and prosecution of the suspected attacker. Based on the extradition rules for this state, the individual would then be either extradited to the victim state for prosecution or prosecuted within the source state under the mutual prosecution agreement. Where possible, the victim nation would finance the requested actions directly so as not to improperly penalize states that did not contribute to the attack.

B. *Concerns that May Arise*

Given the complexity of the problem of cyberattacks, a number of potential concerns arise when considering any solution. These can be broken into two primary areas: concerns about abuse of the system and concerns about the practicality of such a solution.

1. Abuse of the Monitoring System

Any system that increases a government's ability or legitimacy in monitoring the action of citizens inherently creates two problems. First, there are concerns regarding the invasion of personal privacy, and second, there is a potential for a state to abuse such a system. By implementing a system that enables, and often will require, states to monitor activity within their cyberspace, the assumption of anonymity on the Internet quickly fades away. Given this proposal, states without their own monitoring systems may either develop a system independently or utilize the ITU's assistance to develop a system. The ITU's assistance will come in both technical assistance and possibly in providing the physical portion of the system, if financially feasible.

For the nations who utilize the ITU's assistance in developing their domestic framework, the ITU will be granted oversight of the system, including auditing the systems to ensure compliance with limitations in usage. Failure to comply could result in a number of punishments, such as removal from the collective protection afforded by this proposal or disabling the monitoring system from an external kill switch. This would set the nation back to the original status and thus not damage any functions of the state beyond what they had prior to the ITU's assistance. States that currently have their own system in place would not be subject to the ITU audits except to ensure that their system is sufficient. Currently, these states are able to monitor their domestic

Internet,[181] but would be subject to domestic privacy laws and human rights laws should the use of this monitoring service exceed the permissible purposes.[182] Although this allows the states with their own systems to avoid the more stringent restrictions placed upon assisted states, the purpose of this plan is to prevent the ITU from permitting the improper use of ITU installed systems by simply returning the offending state back to pre-ITU assistance status. To infringe on a nation's independently developed system would disproportionately penalize that nation more than states with no system in place. Further, and perhaps more significantly, this proposal would raise awareness to the concerns about the monitoring system, which will help create checks and balances to prevent abuse.[183]

The other concern regarding the abuse of the system is the potential for oppressive governments to utilize these structures for improper purposes. Abuses of Internet rights by oppressive regimes have occurred with significant publicity during the Arab Spring.[184] Oppressive regimes, if they have their own domestic monitoring system in place, would already be able to monitor their populace. This proposal could not stop states from acting outside their laws within their borders with systems they created, but the pressure asserted by the citizenry would place a burden on the state to protect the rights of the citizen. Breaches of these laws are issues for domestic or, if applicable, international courts on a case-by-case basis. Systems, however, would be in place to prevent oppressive regimes from requesting that other nations spy on political dissidents abroad. Here, the ITU can

181. *See NSA Has Access to 75 Percent of US Internet Traffic, Says WSJ*, NBC NEWS (Aug. 21, 2013, 8:03 AM), http://www.nbcnews.com/technology/nsa-has-access-75-percent-us-internet-traffic-says-wsj-6C10967780.

182. *See generally Privacy and Human Rights*, GLOBAL INTERNET LIBERTY CAMPAIGN, http://gilc.org/privacy/survey/intro.html (last visited Aug. 29, 2013).

183. Although cybermonitoring is not an exact match, an apt comparison is wiretapping and the controls placed on those performed against American citizens. In *United States v. United States District Court for the Eastern District of Michigan, Southern Division*, the Supreme Court found that in cases of domestic monitoring, "[o]fficial surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech." 407 U.S. 297, 320 (1972). Because of this, the Court finds that the burden on the government to seek judicial approval when seeking a wiretap is "justified in a free society to protect constitutional values." *Id.* at 321. Thus, when considering the domestic monitoring that would be necessary under this proposal, the requirements imposed on states will create domestic pressures to implement procedures to protect their citizenry in a similar fashion to those afforded to U.S. citizens by the Fourth Amendment, thus making it more difficult to employ in inopportune ways. *Id.*

184. *See, e.g.*, Matt Richtel, *Egypt Cuts Off Most Internet and Cell Service*, N.Y. TIMES (Jan. 28, 2011), http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html (discussing the Egyptian Internet Shutdown during the Arab Spring).

independently block the request when first submitted or block it through a secondary review after an ITU-C review requested by a member state. At minimum, this presents a barrier to, if not prevents, the completion of improper requests.

2. Practicality

From a practical perspective, two issues arise. The first issue is why states should agree to adopt the additional optional protocol expanding the ITU, and second, how the ITU and the information requests would be funded. When adopting the additional protocol, each state must consider a number of factors. First, as cyberattacks become an increasing threat to all nations,[185] the ability to attribute an attack is the core of any solution. The ability to attribute an attack will help prevent attacks through stronger enforcement of cyber laws and punishment. If it becomes nearly impossible to attribute an attack, then individuals may carry out cyberattacks with impunity. Additionally, being able to attribute and hold an individual responsible for an attack decreases the risk of cyberweapons being the catalyst for World War III. The U.S. assertion that kinetic weapons can be used to protect its cyberspace will still hold true, but other forms of holding the responsible party liable will discourage the use of weapons except in the most severe circumstances.

This solution will also provide assistance to states to secure their cyberborders. States who currently do not have a structure in place to protect their cyberrealm will gain significant benefits through a new system. The states that already have a system will gain the benefit of collective monitoring through the ability to request assistance from other states to determine the attack's source. Given increased interactions and norms developed through this framework, nations will become familiar with the procedures and actions needed, preparing them to respond quickly to attacks, provide vital information, and even potentially stop an attack prior to a catastrophic result. Further, this norm creation may assist in developing a stigma against the use of cyberweapons, potentially driving a shift toward defensive actions and heading off a cyberarms race before it can fully develop.[186] Should any

185. *See Cyber Threats to Increase in 2012: Report*, TIMES INDIA (Oct. 12, 2011, 6:58 PM), http://articles.timesofindia.indiatimes.com/2011-10-12/internet/30270474_1_mobile-web-threats-internet-users.

186. *See 57% Believe a Cyber Arms Race is Currently Taking Place, Reveals McAfee-Sponsored Cyber Defense Report*, BUSINESS WIRE (Jan. 30, 2012, 11:01 AM), http://www.businesswire.com/news/home/20120130005063/en/57-Cyber-Arms-Race-Place-Reveals-McAfee-Sponsored (discussing study of opinions on the cyberarms race today).

nation opt out of this program, it will weaken the ability of the ITU to carry out its functions effectively. Through collaboration, the international community must produce significant pressure on any belligerent nation to ensure effective protection.

Because this proposal calls for the expansion of an organization that already exists, much of the core structure of the ITU's funding system is already in place. This structure relies upon membership fees.[187] To acquire funds for the increased role, the fees on each nation would increase to enable the structural expansion of the organizations. The cost for assisting in developing individual cybermonitoring tools in states that request this support would be partially offset from the increased experience with the ITU-D, requiring only one additional step when aiding the nation in developing the cybermonitoring tools. While there will invariably be significant costs when the program is launched, the largest costs of assisting states within the system are one-time costs. Within short order, states will see benefits outweighing their costs as cyberattacks will drop. The individual state retains the burden of responding to attacks in their territory. So when a state requests assistance in investigating an international attack, the state requesting the investigation will be required to pay the costs of the investigation, preventing member states from assuming costs beyond the benefits afforded to them.

VI. CONCLUSION

As the Internet becomes increasingly crucial to everyday life, the potential for catastrophic cyberattacks on the Internet and the systems reliant upon it grows. Cyberattacks have continued to increase in frequency, brazenness, and impact, yet the ability for individual nations to attribute the attack has failed to similarly grow. Consequently, because the Internet is innately an international structure, solely domestic solutions will continue to be inadequate; an international response is essential. A failure to act will fundamentally ensure that a cyberattack will be launched, which will result in a loss of life due to the disabling of vital infrastructure or the launching of a kinetic war.

To address the issue of cyberattacks, this proposal sets forth a dual-pronged approach. The two changes will alter the responsibilities of the ITU and the individual states. The expansion of the ITU's organizational mandate and structure will enable the ITU to address the issue of cyberattacks. States will face a shift in their role as well. First, the state will be liable for cyberattacks by individuals within their

187. *See Membership*, *supra* note 167.

borders in a system that replicates the Bush Doctrine. A state can escape liability using domestic cybermonitoring systems to investigate the attack and then prosecute or extradite. With these elements in place, the victims will be able to hold the responsible party accountable for the cyberattacks, thus creating a deterrent for cyberattackers.