American University International Law Review

Volume 17 | Issue 3 Article 4

2002

A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China

Daniel M. Creekman

Follow this and additional works at: http://digitalcommons.wcl.american.edu/auilr

 Part of the International Law Commons

Recommended Citation

Creekman, Daniel M. "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China." American University International Law Review 17, no.3 (2002): 641-681.

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University International Law Review by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact fbrown@wcl.american.edu.

A HELPLESS AMERICA? AN EXAMINATION OF THE LEGAL OPTIONS AVAILABLE TO THE UNITED STATES IN RESPONSE TO VARYING TYPES OF CYBER-ATTACKS FROM CHINA

DANIEL M. CREEKMAN*

---

* J.D. Candidate, 2003, American University, Washington College of Law; B.A. Political Science, Davidson College. I would like to thank my parents, Jim and Virginia Creekman, grandmother, Mrs. Louise Prince, and brother David for their unwavering love, support, and encouragement, not only through law school, but throughout my life. This Comment would not have been possible without the help of the entire INTERNATIONAL LAW REVIEW staff, especially my editors Jeremy Frey and Michael Haas. A final thank you is owed to Ms. Beth Ann Barozie for her assistance, encouragement, and sense of humor from deciding on a topic to the final edit.

INTRODUCTION

For at least half of the past century, America routinely conducted surveillance flights over the People's Republic of China[1] in order to gain valuable electronic and visual intelligence that is unobtainable by the fleet of satellites orbiting in space.[2] Though largely unreported to the American public, the Chinese government recently began sending jet fighters to shadow, or intercept, the cumbersome reconnaissance planes.[3] On April 1, 2001, these flights garnered worldwide attention when an American EP-3E Aries II surveillance plane collided with a Chinese F-8 fighter about seventy miles off the coast of China.[4] The collision severed the nosecone from the American plane and sent it plunging into an 8,000-foot freefall culminating in an emergency landing at a Chinese airfield on Hainan Island.[5] The Chinese plane, along with its pilot, Wang Wei, spun out of control and was lost at sea.[6]

---

1. *See* Thomas E. Ricks, *Anger Over Flights Grew In Past Year; Proximity Riled China; U.S. Cited Interceptors*, WASH. POST, Apr. 7, 2001, at A1 (describing surveillance flights along the Chinese coast in early 1960); *see also* Steven Lee Myers, *Collision With China: The Pentagon; U.S. Tape Is Said to Show Reckless Flying by Chinese*, N.Y. TIMES, Apr. 13, 2001, at A6 (noting Secretary of Defense Donald Rumsfeld's comments that the United States routinely conducted surveillance flights over China for years).

2. *See* Ricks, *supra* note 1, at A1 (quoting a retired naval expert that the purpose of the surveillance flights is to obtain the electronic emissions and visual images that satellites can not get because they can not be overhead all of the time).

3. *See* Neil King Jr. et al., *China Refuses to Release U.S. Spy Plane, Crew*, WALL ST. J., Apr. 3, 2001, at A16 (indicating China's recent practice of using fighter jets to intercept U.S. reconnaissance planes); *see also* Ricks, *supra* note 1, at A1 (stating that the Chinese launch their fighter jets to intercept close to one out of every three reconnaissance flights and this rate has remained constant as the United States increased the number of flights it has conducted).

4. *See* Nancy Gibbs & Michael Duffy, *Bush's Big Test*, TIME, Apr. 16, 2001, at 24 (detailing the events leading up to and following the midair collision of the two planes).

5. *See* Evan Thomas & Melinda Liu, *A Crash In the Clouds: The Dogfight*, NEWSWEEK, Apr. 16, 2001, at 26 (describing the midair collision and subsequent events).

6. *See id.* (noting that there were reports that the Chinese pilot bailed out, and was apparently lost at sea).

As American officials worked to obtain the release of the detained crew and airplane, the two countries publicly blamed each other for causing the crash.[7] Meanwhile, tech-savvy American citizens, angry over the detention of the EP-3 crew, expressed their outrage through threats and "trash talking" over the Internet as they defaced or vandalized at least sixty-five Chinese websites.[8]

In response, a group of Chinese hackers, calling themselves the Hackers Union of China or the Honkers Union of China,[9] declared war on their American counterparts.[10] Pronouncing the week of May 1 through May 7, 2001 as "Hack the USA" week,[11] the Honkers

---

7. *See, e.g.*, Erik Eckholm, *Collision With China: The Reaction; Angry Beijing Denounces Washington's Reports That Its Pilot Caused the Collision*, N.Y. TIMES, Apr. 15, 2001, at A10 (reporting the Chinese government's response to statements made by the U.S. government that the Chinese version of events was incorrect and the Chinese pilot had, in fact, caused the crash). The Chinese asserted that the American plane abruptly turned into the path of the Chinese fighter, causing the collision. *See* Steven Mufson & Philip P. Pan, *Spy Plane Delays Irk President; Bush Asks 'Prompt' Release by Chinese*, WASH. POST, Apr. 3, 2001, at A1. The United States, however, stated that it was "inconceivable that the slower moving, propeller-driven U.S. plane could have cut off the nimble fighter." *Id.* Instead, Pentagon officials said that the evidence suggests two possible scenarios, both of which implicate the Chinese pilot and suggest that his aggressive, "flashy" intercept tactics brought his fighter within 10 feet of a surveillance flight in a previous, documented encounter. *See* Stephen Lee Myers, *Collision With China: Washington; Chinese Pilot Reveled in Risk, Pentagon Says*, N.Y. TIMES, Apr. 6, 2001, at A1.

8. *See* Malcolm Beith, *The U.S.-China Hacker Conflict*, NEWSWEEK, May 7, 2001, at 5 (describing the then recent Chinese cyber-attacks as retaliation for attacks made by American hackers); *see also Hackers Report a Truce*, N.Y. TIMES, May 10, 2001, at A11 (reporting the "cyberwar" between Chinese and American hackers that began after American hackers mounted a cyber-attack in response to the collision of the two countries' planes); *see also* Chris Farnsworth, *U.S.-China "Cyberwar" Fallout is Felt in O.C.*, ORANGE COUNTY REG., May 9, 2001, at 1 (attributing the start of the cyberwar to the "trash talk" and racial slurs American hackers put on Chinese websites in response to the crash).

9. *See* Ariana Eunjung Cha, *Chinese Suspected of Hacking U.S. Sites; Anger Over Plane Collision Calls for Revenge, Advice on Web Attacks*, WASH. POST, Apr. 13, 2001, at A13 (reporting the name of the group claiming credit for many of the recent website hackings).

10. *See* Elizabeth Becker, *F.B.I. Warns That Chinese May Disrupt U.S. Web Sites*, N.Y. TIMES, Apr. 28, 2001, at A8 (stating that the F.B.I. issued a warning that Chinese hackers might organize and increase their attacks on American websites).

11. *See* Michelle Kessler, *China Troubles Linked to Attacks on Web Sites Run*

Union took credit for shutting down or altering multiple government websites, including the websites for the Office of the Clerk of the United States House of Representatives[12] and the White House.[13] The hackers replaced the content of one site with China's fluttering red flag and a rendition of the Chinese national anthem that automatically played whenever users accessed the site.[14] Hackers replaced other sites with tributes to Wang Wei,[15] the dead Chinese pilot, or plastered the sites with messages such as "Beat Down Imperialism of America" and other anti-American, pro-Chinese sentiments.[16] The hackers ended their war after claiming to have hacked one thousand American websites.[17] Several commentators,

---

By U.S. Government, USA TODAY, May 2, 2001, at 6B (describing several attacks on U.S. websites as part of an organized protest movement against the plane collision incident as well as the accidental U.S. bombing of the Chinese embassy in Belgrade, Yugoslavia that occurred on May 7, 1999). In addition to encompassing the anniversary of the embassy bombing, the "Hack the U.S.A." week also coincided with the Chinese holidays of May Day (May 1) and Youth Day (May 4). *See* Riva Richmond, *American Hackers Do Most Damage in China - U.S. "Cyberwar,"* DOW JONES NEWS SERVICE, May 2, 2001.

12. *See* Lauren W. Whittington, *Pro-China Hackers Hit House Clerk's Office*, ROLL CALL, May 3, 2001, at 1 (detailing the damage done to the website of the office of the Clerk of the United States House of Representatives).

13. *See* Craig S. Smith, *The First World Hacker War*, N.Y. TIMES, May 13, 2001, at D4 (describing the cyber-attacks on the White House, the California Department of Justice, and an Eastern Ohio School District's website or computer system).

14. *See id.* (describing damage done to the website of eastern Ohio's Bellaire School District).

15. *See Chinese Hackers Invade 2 Official U.S. Web Sites*, N.Y. TIMES, Apr. 29, 2001, at A10 (reporting that one of the Department of Labor's websites was replaced with an homage to the pilot and that two sites run by the Department of Health and Human Services were altered and taken offline).

16. *See* Sam Costello, *U.S., Chinese Hackers Continue Web Defacements*, INFOWORLD DAILY NEWS, May 1, 2001 (stating that the sites attacked by the Chinese hackers included the U.S. Geological Survey, Eastern Region, the Hurricane Liaison Team of the Federal Emergency Management Agency, and the headquarters of the Commander of the Naval Surface Force of the U.S. Atlantic Fleet).

17. *See* Smith, *supra* note 13, at D4 (noting that the Chinese hackers called off their attacks a day after China's Communist Party newspaper called the attacks "unforgivable"); *see also* Robert MacMillan, *Chinese Crackers Call Off Crusade*, NEWSBYTES NEWS NETWORK, May 9, 2001 (reporting the announcement by the Chinese hackers to end the attacks after reaching their goal of hacking one

however, speculated the Chinese government was actually responsible, even though there was nothing to controvert the Honkers Union's claims of credit for the attacks.[18]

The actual identity of the perpetrators was ultimately irrelevant, however, since there was an absence of accountability throughout the "cyberwar" and its aftermath.[19] Individuals and groups claimed credit for successful hacks with impunity.[20] None of the articles reporting the battle of words over the Internet mentioned any consequences or remedies for the victims, some of whom were private companies.[21] Other than the diplomatic implications, it did not seem to matter whether or not the Chinese government was responsible.[22] While the lack of penalties, or even contemplated penalties, may be common for such insignificant damages,[23] it raises the question of how the United States would respond if the damage was worse or the targets more vital.[24] For example, what if Chinese hackers crippled the air-

---

thousand U.S. websites, including sites run by the Inter-American Defense Board, the Federal Highway Administration, and the U.S. Fish and Wildlife Service).

18. *See U.S./China Tit-for-Tat Hacks Escalate*, NEWSWIRE (VNU), May 1, 2001 (noting risk management firms such as iDefense were releasing reports suggesting that the attacks on U.S. websites were state-sponsored since the Chinese government controls so much of its citizen's access and use of the Internet); *see also* Becker, *supra* note 10, at A8 (indicating some American officials, including a member of the advisory board of the National Security Agency, believed the attacks were abetted by the Chinese government). *But see* Ted Bridis, *U.S., Chinese Hackers Infiltrate Web Sites, Trade Insults Across Pacific in "Net War,"* WALL ST. J., May 1, 2001, at B6 (citing U.S. officials as stating there was no evidence of coordination by the Chinese government).

19. *See supra* notes 8-18 and accompanying text (describing the "cyberwar" but making no mention of any sort of penalties or legal actions).

20. *See e.g.*, Carrie Kirby, *Click and Bicker: U.S. and Chinese Hackers Explain Their Online War of Words*, S.F. CHRON., May 8, 2001, at B1 (interviewing four anonymous hackers, two American and two Chinese, involved in the "cyberwar").

21. *See, e.g.*, Farnsworth, *supra* note 8 (describing the damage done to a website of a local manufacturer of soaps and beauty products).

22. *See, e.g.*, Becker, *supra* note 10, at A8 (suggesting Chinese government involvement with no mention of the consequences).

23. *See* Kirby, *supra* note 20, at B1 (stating that the "online spat" between American and Chinese hackers "left little real damage in its wake").

24. *Compare id.* (reporting the victims of the "cyberwar" to be "a few government sites in both countries and a number of small, obscure businesses," including the Bubbles carwash in Houston and Jianlong Decorative Materials Factory in China's Guangdong province) *with* Andrea Stone, *Cyberspace is the*

traffic controller computer systems at major U.S. airports,[25] or disabled the computers running the New York Stock Exchange?[26] Given the potentially catastrophic consequences, the identity of the perpetrator, as well as the need to bring that perpetrator to justice, is of paramount importance. This is especially vital when an attack on a critical U.S. infrastructure by a foreign government could ultimately result in war.[27]

This Comment analyzes the different legal responses available to the United States and its citizens to different levels of Chinese[28] cyber-attacks, ranging from website vandalism by Chinese individuals, to organized attacks on vital U.S. systems orchestrated by the Chinese government in lieu of a traditional military confrontation. Part I describes the different types of attacks, their consequences, and some of the instruments used to achieve them. In addition, Part I establishes and defines the four different types of attacks. Part II examines the available legal responses to each type of attack. This analysis includes a review of U.S., Chinese, and international law in terms of how each treats computer crimes and

---

Next Battlefield U.S., Foreign Forces Prepare for Conflict Unlike Any Before, USA TODAY, June 19, 2001, at A1 (contending that serious cyber-attacks on the United States could include, among other things, instruments that would shut down power grids in major cities, and flood the Hoover Dam).

25. *See* M.E. Bowman, *Is International Law Ready For the Information Age?*, 19 FORDHAM INT'L L.J. 1935, 1939 (1996) (offering the Federal Aviation Administration's air-traffic control system as a potential and vulnerable target for a computer attack).

26. *See* Michael Specter, *The Doomsday Click*, NEW YORKER, May 28, 2001, at 110 (commenting on the potential for terrorists to wage economic warfare by unplugging the Federal Reserve system from Wall Street).

27. *See generally* Todd A. Morth, Note, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, 30 CASE W. RES. J. INT'L L. 567 (1998) (arguing information warfare, or attacks on information networks should be treated as a use of force internationally prohibited under section 2(4) of the U.N. Charter). If the attack is severe enough, the victim is entitled to respond in self-defense, establishing a course of action that could culminate in war. *See infra* notes 154-169 and accompanying text (discussing the use of force in self defense); *see also* Warren P. Strobel et al., *A Glimpse of Cyberwarfare*, U.S. NEWS & WORLD REP., Mar. 13, 2000, at 32 (citing a Russian general, through a senior CIA official, that equated the effects of a cyber-attack on a transportation or electric grid to those of a nuclear blast).

28. *See infra* notes 45-63 and accompanying text (detailing the reasons for focusing the discussion on attacks originating from China).

attacks. Finally, Part III recommends specific improvements that could better protect and police both private and government computer systems in order to prevent and respond to these types of attacks.

I. BACKGROUND

A. THE INTERNET AND HACKING

The Internet, which began as an obscure military experiment in 1968,[29] has become so entrenched in society that by 1999, nearly sixty-eight million Americans had either been online or used the Internet.[30] Unfortunately, along with this widespread use and dependence comes widespread risk and liability.[31] Although the Internet and computers revolutionized most of America's infrastructure, they also placed that infrastructure at considerable risk to a debilitating computer attack.[32] In addition, the explosion of

---

29. *See* Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet*, 50 FED. COMM. L.J. 117, 119 (1997) (describing the rapid growth and expansion of the Internet from its beginnings as a military experiment). The Internet, as it is known today, arose from ARPAnet, the result of a project by the then Advanced Research Projects Agency to build a computer network resilient to physical attacks or malfunctions in part of the system. *See* PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURE; THE REPORT OF THE PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, 16-17 (1997) [hereinafter PCCIP Report], *available at* http://www.ciao.gov/PCCIP/PCCIP_Report.pdf (last visited Sept. 18, 2001).

30. *See* Frank J. Cilluffo et al., *Bad Guys and Good Stuff: When and Where Will the Cyber Threats Converge*, 12 DEPAUL BUS. L.J. 131, 140 (1999/2000) (citing various statistics indicating the rapid growth and widespread use of the Internet, including the fact that nearly ninety percent of large companies and seventy-five percent of small companies now use local area networks for their businesses).

31. *See, e.g.*, PCCIP Report, *supra* note 29, at 9 (predicting that nineteen million individuals worldwide will have the skills to launch a cyber-attack by 2003).

32. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 896 (1999) (citing a theoretical list of "Top 10" Information

computer technology increased the tools available for criminals to commit crimes such as theft and fraud.[33] While there are many computer related offenses,[34] this Comment focuses on hacking—the illegal entry into a computer system[35]—and the havoc and destruction a hacker can cause.

Computer hacking is becoming more widespread and no longer requires an advanced education, as demonstrated by the hacking wars over the EP-3 incident.[36] Step-by-step hacking instructions are easily obtainable on the Internet.[37] While hacking into another computer is generally considered trespassing in the United States and carries its own punishments under the Computer Fraud and Abuse Act ("CFAA"),[38] most experts are more worried about the damage the

---

Warfare targets including the electric switch system handling all federal funds and transactions, the electrical switch system that manages all telephones, the Internet, the time distribution system, and the Panama Canal). In addition, the list includes the Worldwide Military Command and Control System, the Air Force satellite control network, the Strait of Malacca—which is the major maritime link between the Europe-Arabian peninsula and the Western Pacific and East Asia—the Alaska pipeline, and the National Photographic Interpretation Center. *See id.*

33. *See, e.g.*, Laura J. Nicholson et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207 (2000) (examining various types of computer crimes and applicable laws and statutes).

34. *See generally* John T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. 317, 331-59 (1997) (detailing different categories of computer related offenses ranging from child pornography and pedophilia to hacking and computer theft).

35. *See id.* at 346 (defining hacking as involving illegal entry into a computer system).

36. *See* Specter, *supra* note 26, at 115 (describing the ease with which it is possible to hack into a computer).

37. *See id.* at 120 (demonstrating how, with a few clicks of the mouse on a cyber-café computer, the author was able to create a virus as destructive as the Kournikova virus). Meanwhile, the hackers the author was interviewing were accessing the database of the Los Angeles Police Department as well as gathering the names and credit card information from the largest Internet-service provider in the Netherlands. *See id.*

38. 18 U.S.C. § 1030 (1994) (responding to Congress' need to regulate the Internet). After several amendments and rewrites, sections of the Computer Fraud and Abuse Act ("CFAA") were amended by the National Information Infrastructure Protection Act, Pub. L. No. 104-294, 110 Stat. 3488, 3491-94 (1996); *see also* Soma et al., *supra* note 34, at 347-48 (discussing the CFAA as it relates to unauthorized access to a computer, and stating that the punishment for pure trespass can be up to six months in prison in some countries). *See generally*,

hacker can cause after gaining access, rather than the hack itself.[39] The damage usually results from the release of rogue programs distributed by the hacker such as viruses,[40] worms,[41] time (or logic) bombs,[42] or Trojan horses,[43] each of which have the potential to completely disable an individual computer or an entire computer system.[44]

B. WHY CHINA?

The easy availability of the tools needed to instigate a cyber-attack, namely a computer and a modem, mean that an attack could originate from literally any place in the world by any person in the

---

Nicholson et al., *supra* note 33, at 212-16 (analyzing the offenses under the National Information Infrastructure Protection Act ("NIIPA")).

39. *See* Soma et al., *supra* note 34, at 349 (detailing the ways a hacker can damage a computer or system once inside).

40. *See id.* (defining a virus as a computer program with the potential to spread between computers without human intervention by using each newly infected computer to replicate itself). Viruses can be benign and may, for example, cause the computer to display a ridiculous message, or the virus can be malignant and alter or destroy programs and data on the infected computer. *See id.*

41. *See id.* at 350 (defining computer worms as programs that crawl through infected computers, occupying valuable storage space by repeatedly copying themselves, which can potentially crash the system); *see also* Robert J. Malone & Reuven R. Levary, *Computer Viruses: Legal Aspects*, 4 U. MIAMI BUS. L.J. 125, 135 (1994) (describing the IBM Christmas card worm that started in West Germany, crossed the Atlantic, and eventually caused the three-day closing of IBM's internal mail system).

42. *See* Soma et al., *supra* note 34, at 350 (describing both time bombs and logic bombs as viruses that lay dormant until a specific time). The difference between the two bombs is that time bombs are executed at a pre-set date, while logic bombs are triggered by the occurrence of a predetermined event. *See id.; see also* Malone & Levary, *supra* note 41, at 136-38 (detailing a time bomb, the Israeli, or Friday the 13th Virus, that was programmed to erase all the files in the infected computer on Friday, May 13, 1988, as well as a logic bomb, the Scores Virus, that activated whenever it discovered proprietary information of a certain company and proceeded to erase all of that information).

43. *See* Malone & Levary, *supra* note 41, at 139 (explaining Trojan horses as benign programs that contain hidden and destructive programs). An example of a Trojan horse would be a program for a chess game that also contains a hidden virus, so that whenever the innocuous chess game is downloaded, the virus is spread. *See id.*

44. *See* Soma et al., *supra* note 34, at 349 (describing the damage rogue programs can cause to computers).

world.[45] While many of the broader, theoretical issues implicated in a discussion of computer attacks remain constant regardless of the perpetrator,[46] many of the decisions regarding an appropriate response are dictated by the specific circumstances surrounding the attack.[47] With this in mind, this Comment concentrates its discussion on attacks originating from a single country in order to offer a practical application and perspective.[48]

Specifically, this Comment focuses on China because of the unique issues surrounding Sino-American relations,[49] as well as the relevance of such a discussion to recent events.[50] Since the brutal suppression of pro-democracy protesters in China's Tiananmen Square in 1989, the relationship between the United States and China has reached a point of "deep, mutual ambivalence" bordering on

---

45. *See* Schmitt, *supra* note 32, at 897 (dubbing computer attacks "war on the cheap" and citing one expert as claiming that with one million dollars and twenty individuals he could "bring the U.S. to its knees"); *see also* Michael J. Robbat, Note, *Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm*, 6 B.U. J. SCI. & TECH. L. 10, 8 (2000) (presenting computer attacks as the "great equalizer" for militarily inferior nations and groups). Thus, the threat of computer attacks is greatly magnified due to the low cost and wide availability of the tools needed to conduct such an attack. *See id.*

46. *See, e.g., infra* notes 154-177 and accompanying text (describing the implication of the law of conflict management and what factors are considered in determining an appropriate and legal responsive use of force).

47. *See, e.g., infra* notes 88-105 and accompanying text (setting forth the difficulties the United States would encounter in arresting a computer hacker residing in a country with which the United States does not have an extradition treaty).

48. *See supra* notes 45-47 and accompanying text (acknowledging that while many of the issues regarding a computer attack may be the same, any response to a computer attack will be dictated by the specific circumstances surrounding that attack, especially the different nations involved). For example, an attack originating from a perpetrator in England would warrant a much different response and involve different issues than would an attack from a perpetrator in China, primarily because of the absence of an extradition treaty with China. *See infra* notes 91-92 and accompanying text (explaining the implications for the United States of not having an extradition treaty with China).

49. *See generally infra* notes 50-63 and accompanying text (detailing the unique situation between China and the United States).

50. *See supra* notes 1-27 (describing the surveillance plane incident between the United States and China, and subsequent website defacements exchanged over the Internet between the citizens of these two countries).

distrust.[51] China's continual rapid growth in the past twenty years, both economically and militarily,[52] means that the United States is still not certain whether it faces an emerging superpower that challenges U.S. security and economic interests, or a reform-minded developing country.[53] Similarly, China is equally ambivalent towards the United States. They understand that the United States is important for their development, yet also an obstacle to their ascension as an international power.[54] China is eager to engage in constructive, bilateral relations with the United States, but at the same time is deeply suspicious of U.S. intentions toward China and any increase in U.S. global influence.[55] China's size, Security Council membership, nuclear capabilities, massive economy and military strength, and its increased diplomatic presence, requires that the United States interact with China.[56] Unfortunately, the terms of

---

51. *See* DAVID M. LAMPTOM, SAME BED, DIFFERENT DREAMS: MANAGING U.S.-CHINA RELATIONS, 1989-2000 16 (2001) (discussing the seminal events since 1989 that have shaped the current relationship between the United States and China, and describing that relationship as being dominated by ambivalence and possible distrust).

52. *See* CHEN JIAN, THE CHINA CHALLENGE IN THE TWENTY-FIRST CENTURY: IMPLICATIONS FOR U.S. FOREIGN POLICY 1 (1998) (commenting on China's rapid growth and describing it as nothing short of phenomenal).

53. *See* Richard H. Solomon, *Foreword* to CHEN JIAN, THE CHINA CHALLENGE IN THE TWENTY-FIRST CENTURY: IMPLICATIONS FOR U.S. FOREIGN POLICY, at vii (1998) (indicating U.S. uncertainty toward China). This dilemma is often characterized as whether the United States is facing a "China Threat" or a "China Challenge." *See* JIAN, *supra* note 52, at 1.

54. *See Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 107th Cong. 58 (2001) (statement of Thomas Fingar, Acting Assistant Secretary of State for Intelligence and Research) (responding with the word "ambivalent" to a question regarding the attitude of Chinese leaders towards the United States). *See generally* LI DAOYU, *The View From China*, *in* PREPARING AMERICA'S FOREIGN POLICY FOR THE 21ST CENTURY 43, 44-46 (David L. Boren and Edward J. Perkins eds., 1999) (articulating China's view of the United States).

55. *See Statement of the Director of Central Intelligence George J. Tenet as Prepared for Delivery Before the Senate Armed Services Committee Hearing on Current and Projected National Security Threats*, *in* CYBER TERRORISM AND INFORMATION WARFARE II: U.S. EXECUTIVE AND CONGRESSIONAL PERSPECTIVES 77, 84-85 (Yonah Alexander and Michael S. Swetnam eds., 1999) (testifying about the threat China poses to the national security of the United States).

56. *See A Reexamination of U.S.-China Relations: Hearing Before the Subcomm. on E. Asian and Pac. Aff. of the S. Comm. on Foreign Relations*, 106th

that relationship are still unclear.[57] Thus, a discussion of a cyber-attack originating from China becomes especially interesting because of the ambivalence already surrounding relations between the two countries.[58]

In addition, focusing the current discussion on cyber-attacks from China has a certain relevance in light of the incidents subsequent to the collision of the American EP-3 surveillance plane and Chinese fighter jet.[59] Furthermore, China is one of a limited number of countries whose military is specifically exploring the incorporation of computer attacks into their broader military doctrine and strategy.[60] In fact, the Chinese government has gone so far as to contemplate the development of a fourth branch of their military

---

Cong. 3-4 (1999) (statement of Hon. Stanley O. Roth, Assistant Secretary of State for East Asian and Pacific Affairs) (indicating that China's circumstances require that the United States deal with China by stating that "[i]t is not a question of engaging or not engaging").

57. *See generally* JIAN, *supra* note 52, at 16-23 (detailing the difficulties faced in defining Sino-American relations); John T. Rourke & Richard Clark, *Making U.S. Foreign Policy Toward China in the Clinton Administration*, *in* AFTER THE END: MAKING U.S. FOREIGN POLICY IN THE POST-COLD WAR WORLD 201 (James M. Scott ed., 1998) (describing the challenges faced by the Clinton Administration in formulating a foreign policy towards China); Henry A. Kissinger, *The Architecture of an American Foreign Policy for the Twenty-first Century*, *in* PREPARING AMERICA'S FOREIGN POLICY FOR THE 21ST CENTURY, *supra* note 54, at 299, 302-03 (discussing America's foreign policy into the twenty-first century, with special attention to the challenges associated with China); Zbigniew Brzezinski, *A Geostrategy for Eurasia*, *in* PREPARING AMERICA'S FOREIGN POLICY FOR THE 21ST CENTURY, *supra* note 54, at 309, 314-16 (setting forth a foreign policy strategy for relations with European and Asian countries, especially China).

58. *See supra* notes 51-57 and accompanying text (elaborating on the issues surrounding U.S.-China relations).

59. *See supra* notes 1-27 and accompanying text (describing the surveillance plane incident and the trading of website defacements and insults over the Internet between Chinese and American citizens prior to the release of the American crew).

60. *See* National Communications System, Office of the Manager, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document*, *in* CYBER TERRORISM AND INFORMATION WARFARE I: ASSESSMENT OF CHALLENGES 343, 384 (Yonah Alexander & Michael S. Swetnam eds., 1999) (including China, along with Russia, South Korea, Cuba, Japan, Germany, France, Iraq, Israel, and Bulgaria, as a country currently incorporating computer attacks into its military strategies and doctrine).

dedicated to computer and Information Warfare ("IW").[61] In addition, they are recruiting civilian hackers and training them at Army schools to create a cadre of "cyber warriors."[62] Analyzing cyber-attacks originating specifically from China offers a more focused and practical discussion with real world application and relevance as well as one permeated with interesting, difficult, and unique issues in terms of feasible American responses to cyber-attacks.[63]

C. TYPES OF ATTACKS

Naturally, the list of feasible responses depends on the nature of the initial attack, with different attacks implicating different types of responses.[64] One of the distinguishing features between the different types of attacks is whether the attacker is a private citizen or acting at the direction of a government.[65] This distinction is critical because it determines which body of law controls any subsequent response.[66] A response made by a State against a non-state actor, especially a private citizen, is generally a law enforcement matter.[67] Thus, if the non-state actor is not a citizen of the responding State, and therefore not subject to that State's jurisdiction, the responding State must comply with current bilateral and multilateral extradition and legal

---

61. *See infra* notes 179-180 and accompanying text (describing China's dedication to the use of computer attacks as a viable military option).

62. *See infra* note 178 and accompanying text (highlighting China's efforts to strengthen its computer capabilities in terms of military strategy).

63. *See generally supra* notes 45-64 and accompanying text (explaining the reasons for focusing this Comment specifically on cyber-attacks originating in China).

64. *Compare infra* notes 88-119 and accompanying text (discussing the available legal responses to a cyber-attack on a non-vital target by a private citizen), *with infra* notes 178-194 (analyzing the available legal responses to a cyber-attack instigated by a nation-state against a vital target).

65. *See infra* notes 66-72 and accompanying text (presenting the differing controlling laws as determined by whether or not the attacker is a state actor).

66. *See infra* notes 67-72 (setting forth the two different bodies of law that would control any response depending on the relationship of the attacker to his host nation).

67. *See* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 8 (1999) (indicating that a state's use of force against a non-state actor is an issue handled through law enforcement measures).

assistance agreements.[68] On the other hand, a State responding to the actions of another State is controlled by international law.[69] Assuming the initial computer attack damages its target, the responding State's actions are controlled by the internationally recognized law of conflict management.[70] If the response involves the use of force, the law of armed conflict[71] is also implicated.[72]

The target of the attack is another distinguishing feature that determines the types of available responses.[73] Under international law, use of force by one nation against another may not be of such duration, scope, or intensity as to justify a responsive use of force.[74] In this sense, the target systems of a cyber-attack can be characterized as vital or non-vital targets to help determine the severity of a response.[75] Vital targets are those computer systems related to the five critical infrastructures identified by the President's Commission on Critical Infrastructure Protection ("PCCIP"),[76]

---

68. *See id.* (noting that a state action against a non-state actor must be addressed through extradition and mutual legal assistance agreements).

69. *See* L.C. GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 52 (1998) (stating that international law has historically been concerned with relations between states).

70. *See* SHARP, *supra* note 67 at 7 (defining the law of conflict management as that body of law that "defines and governs the use of force between [S]tates during peacetime"). The law of conflict management remains in place and is applicable even when the law of armed conflict is implicated. *See id.*

71. *See id.* (describing the law of armed conflict as being the body of law that governs state action and conduct during hostilities).

72. *See id.* (setting forth the relationship between the law of conflict management and the law of armed conflict).

73. *Compare infra* notes 88-119 and accompanying text (discussing the responses available to an attack on a non-vital target by a private citizen), *with infra* notes 120-44 and accompanying text (describing the responses to an attack on a vital target by a private citizen).

74. *See* SHARP, *supra* note 67, at 7 (indicating that the scope, duration, and intensity of a use of force determine whether an armed conflict exists as a matter of law).

75. *See infra* notes 77-79 and accompanying text (distinguishing between vital and non-vital targets).

76. *See* PCCIP Report, *supra* note 29, at iii (identifying the members of the President's Commission on Critical Infrastructure Protection, which was charged with assessing the nation's vulnerability to computer attacks and recommending protective measures).

charged with assessing the nation's vulnerability to computer attacks.[77] The Commission determined that the United States has five critical infrastructures—Information and Communications, Physical Distribution, Energy, Banking and Finance, and Vital Human Services—whose incapacity or destruction would cripple the United States's defensive or economic security.[78] For the purposes of this discussion, an attack on a vital target is considered an attack on any combination of these five infrastructures, and an attack on a non-vital target is considered an attack on any target not associated with these five infrastructures.[79]

This Comment, therefore, focuses its discussion on computer attacks on either vital or non-vital targets perpetrated by either private Chinese citizens or the government of China.[80] The Comment assumes that any attack or virus completely debilitates the target system.[81] Furthermore, the Comment assumes that the identity of the

---

77. *See id.* at A-1 (defining the five critical infrastructures).

78. *See id.* (setting forth the five critical infrastructures whose incapacity or destruction would have a debilitating effect on U.S. defense or economic security); *see also* Brian A. Persico, *Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure*, 7 COMMLAW CONSPECTUS 153, 156-60 (1999) (discussing threats to the critical components of the National Information Infrastructure, as specified by the PCCIP Report, and elaborating on what each broad category entails). Telecommunications includes telephone networks, Internet, and personal computers. *See id.* at 157. The Energy Infrastructure refers to electric power systems, and oil and gas refining and transmission facilities in the United States. *See id.* at 160. The Banking and Finance infrastructure includes banks, financial services companies, payment systems, investment companies, and securities and commodities exchanges. *See id.* The Physical Distribution infrastructure encompasses the vast network of highways, rail lines, ports, pipelines, inland waterways, airports and air traffic control systems found throughout the United States. *See id.* at 158-59. The Vital Human Services infrastructure consists of the water supply, emergency services, and government services of the United States. *See id.* at 159.

79. *See supra* notes 73-78 and accompanying text (presenting the significance of the target in terms of determining an appropriate response within the boundaries of the applicable laws).

80. *See supra* notes 45-79 (describing the significance of attributing the attacks to China, as well as the importance of distinguishing between state actors, non-state actors, vital targets, and non-vital targets).

81. *See* 18 U.S.C. § 1030(e)(8)(A) (setting the required damage amount to a minimum of five thousand dollars). The assumption that the attack completely debilitates the target system is made in order to avoid complications arising from

attacker is obtainable[82] and that the attacker is either the Chinese government or a Chinese citizen.[83] Thus, this Comment analyzes the legal options available to the United States in response to each of the following types of computer attacks: an attack on a non-vital target by a private Chinese citizen;[84] an attack on a vital target by a private Chinese citizen;[85] an attack on a non-vital target by the Chinese government;[86] and an attack on a vital target by the Chinese government.[87]

II. ANALYSIS: COMPUTER ATTACKS AND THE AVAILABLE LEGAL RESPONSES

A. PRIVATE CITIZEN HACKER

1. Non-Vital Target

If a Chinese citizen-hacker spreads a virus that erases all files on an infected computer, and that virus spreads throughout the United States, infecting as much as fifty percent of the nation's personal

---

the satisfaction of this subsection of the CFAA. *See also infra* text accompanying note 95 (defining "damage" under the CFAA).

82. *See* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1071-72 (2001) (elaborating on the difficulties in tracing a hacker, which may be the greatest challenge). Unlike traditional crime, the range of suspects in cyberspace crime is enormous. *See id.* at 1071. If any "electronic footprints" can be found, investigators may be able to follow them through various servers, but those footprints usually end with fake email addresses on servers that do not carry any subscriber information; thus, resulting in a dead end. *See id.* at 1072.

83. *See supra* notes 45-63 and accompanying text (indicating the significance of attributing the attacks to the Chinese for the purposes of this discussion).

84. *See infra* notes 88-119 and accompanying text (analyzing computer attacks on a non-vital target by a private Chinese citizen).

85. *See infra* notes 120-144 and accompanying text (assessing the responses available to a computer attack on a vital target instigated by a private Chinese citizen).

86. *See infra* notes 144-178 and accompanying text (discussing computer attacks made by the Chinese government on non-vital American targets).

87. *See infra* notes 178-195 and accompanying text (describing attacks on vital targets made by the Chinese government).

computers,[88] there are few legal recourses available to the victims.[89] Prosecuting an American citizen-hacker for spreading a virus throughout the United States is difficult enough,[90] but the absence of an extradition treaty with China renders the prosecution of a Chinese citizen-hacker in U.S. courts nearly impossible.[91]

The American citizen-hacker could be prosecuted for damages caused, as well as the knowing transmission of a program that causes damage,[92] under several subsections of the CFAA.[93] Congress drafted section 1030(a) of the CFAA, for example, to specifically address the type of computer crime described in the hypothetical at the beginning of this section.[94] Depending on how the hacker transmits the virus, the hacker could also be liable under section 1030(a)(5)(A) of the CFAA, which prohibits the knowing transmission of a program to intentionally cause damage[95] to a protected computer.[96] The

---

88. *See* PCCIP Report, *supra* note 29, at 9 (estimating the number of targeted personal computers to be five hundred million by 2001).

89. *See infra* notes 90-119 and accompanying text (discussing the inability of the United States to bring to justice any Chinese citizen-hacker).

90. *See* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177 (2000) (analyzing the various U.S. laws applicable to different computer crimes); *see also* Nicholson et al., *supra* note 33 (describing various federal laws proscribing computer crimes).

91. *See* WILLIAM J. CLINTON, LETTER OF TRANSMITTAL OF THE AGREEMENT WITH HONG KONG FOR THE SURRENDER OF FUGITIVE OFFENDERS, S. TREATY DOC. NO. 105-3, at iii (1997) (noting the absence of an extradition treaty between the United States and the People's Republic of China).

92. *See* Sinrod & Reilly, *supra* note 90, at 224-26 (discussing the CFAA as it applies to malicious viruses).

93. *See* 18 U.S.C. § 1030(c) (presenting the punishment for offenses committed under the CFAA).

94. *See* Sinrod & Reilly, *supra* note 90, at 224 (discussing Congress' intent in drafting section 1031(a) of the CFAA).

95. *See* 18 U.S.C. § 1030(e)(8) (defining "damage" as "any impairment to the integrity or availability of data, a program, a system, or information that (A) causes loss aggregating at least $5,000 in value during any one-year period to one or more individuals; (B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals; (C) causes physical injury to any person; or (D) threatens public health and safety").

96. *See* 18 U.S.C. § 1030(e)(2). The statute defines a "protected computer" as:

[A] computer (A) exclusively for the use of a financial institution or the

maximum penalty for such an offense is five years in prison.[97]

With a Chinese citizen-hacker, however, one of the most difficult tasks would be to bring the hacker to the United States to face trial.[98] In *Factor v. Laubenheimer*,[99] the Supreme Court held that the legal right for a country to demand extradition of another country's citizen exists only when it is created by treaty.[100] Because the United States does not usually enter into treaties with countries it considers to be repressive,[101] there is no extradition treaty with China,[102] and thus, no legal ground to demand the extradition of a Chinese citizen-hacker to face an American judge.[103] While the United States could conceivably ask for extradition absent a treaty, the United States' inability to comply with the reciprocity[104] for which China would

---

United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communication.

Id.

97. *See* 18 U.S.C. § 1030(c) (establishing the guidelines for punishment for violation of the statute); *see also* Sinrod & Reilly, *supra* note 90, at 244-25 (applying section 1030(c)of the CFAA to various virus attack scenarios).

98. *See supra* note 91 and accompanying text (noting the absence of an extradition treaty between the United States and China).

99. 290 U.S. 276 (1933) (examining extradition with respect to U.S. law and treaties to which the United States is a party).

100. *See id.* at 287. The Court interprets international law to hold that:

While a government may, if agreeable to its own constitution and laws, voluntarily exercise the power to surrender a fugitive from justice to the country from which he had fled, and it has been said that it is under a moral duty to do so, the legal right to demand his extradition and the correlative duty to surrender him to the demanding country exist only when created by treaty.

Id.

101. *See* LOUIS HENKIN, FOREIGN AFFAIRS AND THE UNITED STATES CONSTITUTION 270 (2d ed. 1996) (stating that "the United States does not commonly conclude treaties with repressive countries").

102. *See supra* note 91 and accompanying text (noting the absence of an extradition treaty between the United States and the People's Republic of China).

103. *See supra* notes 99-101 and accompanying text (attributing the legal authority to extradite to an extradition treaty between two countries).

104. *See* 18 U.S.C. §§ 3183-3184 (1948) (indicating that by law, the United States cannot extradite one of its nationals without a treaty or convention).

undoubtedly ask, would probably mean the Chinese would deny the request.[105]

Another possible method for bringing the citizen-hacker to justice in the United States is through extralegal seizure.[106] In *United States v. Alverez-Machain*,[107] the Supreme Court held that a federal court did not lose jurisdiction over a suspect because that suspect had been abducted from Mexico and brought to the United States for trial without resorting to the extradition treaty between the United States and Mexico.[108] Thus, U.S. officers, private individuals, law enforcement officers, or military units could mount an operation to abduct the hacker from China in order to bring him to justice in the United States.[109] While this approach is a legal option, the international and diplomatic ramifications of an extralegal seizure would be so dramatic, that it renders the possibility merely an academic exercise.[110]

Even though no damages can be awarded, some American victims might take comfort in the fact that the Chinese citizen-hacker could be convicted in China.[111] However, a conviction will only take place

---

105. *See* Soma et al., *supra* note 34, at 322 (discussing the doctrine of reciprocity as it applies to extradition treaties). Historically, before the emergence of formal treaties, extradition generally worked on a reciprocal basis. *See id.* at 320. Without a formal treaty, and ignoring, for the moment, the other numerous foreign policy implications, the United States could, in theory, ask the People's Republic of China for the extradition of the hacker. However, China would then likely ask for the extradition of an American, a request with which the United States could not comply. *See* 18 U.S.C §§ 3183-3184 (prohibiting the extradition of an American citizen without an extradition treaty in place).

106. *See* Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 39 (1996) (discussing the possibility of extralegal seizure to circumvent the absence of an extradition treaty).

107. 504 U.S. 655 (1992).

108. *See id.* at 669-70 (permitting the prosecution of a defendant apprehended through extralegal seizure in spite of an existing extradition treaty).

109. *See* Perritt, *supra* note 106, at 39 (describing the means by which an extralegal seizure may be conducted).

110. *See* SHARP, *supra* note 67, at 8-9 n.14 (commenting that a use of force by a victim State against a non-state actor in the sovereign territory of another State without that State's consent could be considered an unlawful use of force against that State by the victim State).

111. *See infra* notes 112-120 (examining the conditions under which a Chinese

in Chinese courts if the hacker's virus spreads to Chinese computers.[112] The People's Republic of China ("P.R.C.") added computer crimes to the P.R.C. Criminal Code in 1994,[113] making it a crime to delete, alter, or disturb the operation of a computer information system so that it does not operate properly.[114] A serious offense is punishable by up to five years in prison, and an "exceptionally serious" offense is punishable by no less than five years.[115] In addition, the Chinese government proscribed the deletion of, alteration of, or addition to, programs installed in, or processed and transmitted by, a computer system.[116] They also have prohibited the intentional writing or dissemination of computer viruses or other destructive programs that interfere with the normal operation of a computer system.[117] Unfortunately, the United States cannot force the Chinese to prosecute the hacker, nor can it force an extradition of the citizen-hacker.[118] Thus, while the United States and China both have relevant laws, there is no mechanism in place to ensure that those laws are applied to the citizen-hacker attack scenario.[119]

2. Vital Target

The United States is equally restricted in its available responses

---

citizen-hacker would be prosecuted in China).

112. *See* THE 1997 CRIMINAL CODE OF THE PEOPLE'S REPUBLIC OF CHINA art. 286 (Wei Lou trans., William S. Hein & Co., Inc. 1998) [hereinafter P.R.C. Criminal Code] (criminalizing the distribution of a computer virus to Chinese computers).

113. *Computer Security in China*, 7 E. ASIAN EXECUTIVE REP. 10, Jul. 15, 1998 (reporting the addition of computer crimes to the P.R.C. Criminal Code).

114. *See* P.R.C. Criminal Code, *supra* note 112, art. 286 (prohibiting the deletion, alteration, or disturbance of the operation of a computer information system).

115. *See id.* (setting forth the penalty for an "exceptionally serious" offense).

116. *See id.* (criminalizing any manipulation of computer programs installed in, or processed and transmitted by, computer systems).

117. *See id.* (proscribing the creation and distribution of any destructive computer program).

118. *See supra* notes 88-117 and accompanying text (describing the difficulties the United States faces in attempting to bring a Chinese citizen-hacker to justice under U.S. or Chinese law).

119. *See id.* (discussing the current American and Chinese laws concerning computer crimes).

for redress if the Chinese citizen-hacker were to cripple any one of the United States' critical infrastructures.[120] While the effects of such an attack could be catastrophic,[121] the United States is largely paralyzed in its response because the culprit is a private citizen, and therefore, any response is a law enforcement issue.[122] As such, the absence of an extradition treaty with China[123] again significantly limits the retributive responses available to the United States government and the victims.[124]

Regardless of the specific vital target or the damage that occurs, if a computer attack is attributable only to a private citizen and no connection or sponsorship by any State is determined, the attack must be considered a criminal matter.[125] Like a computer attack on a non-vital U.S. target by an American citizen-hacker,[126] an attack on a vital U.S. target would be controlled by the CFAA.[127] The statute specifically deals with computer–related threats to national security.[128] In addition, the statute prohibits the causation of damage

---

120. *See infra* notes 121-144 and accompanying text (setting forth the available legal remedies to an attack on a vital target by a Chinese citizen-hacker); *see also supra* notes 77-78 and accompanying text (defining vital targets).

121. *See* Strobel et al., *supra* note 27, at 32 (equating the potential destruction a debilitating computer attack could cause to a nuclear explosion).

122. *See* SHARP, *supra* note 67, at 8 n.14 (noting that while a non-state actor and a state actor may cause identical damage to a State's infrastructure, any action conducted by a non-state actor remains a law enforcement issue).

123. *See supra* notes 98-110 and accompanying text (discussing the absence of an extradition treaty with China and the resulting difficulties in attempting to bring a Chinese citizen before an American court).

124. *See id.* (articulating the United States's available responses to a cyber-attack from a Chinese citizen-hacker).

125. *See* Lawrence T. Greenberg et al., *Information Warfare and International Law* ch. 3 (1998) (describing the options available to a State victimized by a crippling computer attack perpetrated by a single individual as unsettled and potentially unsatisfactory because of the necessity of treating the incident as a criminal matter and the subsequent reliance on international treaty law), *available at* http://www.dodccrp.org/iwilchapter3.htm (last visited Oct. 29, 2001).

126. *See supra* notes 92-97 and accompanying text (discussing the possible legal responses available to an attack on a non-vital target by an American citizen-hacker).

127. *See* 18 U.S.C. § 1030 (describing the targets that are vital to the U.S. government).

128. *See* Soma et al., *supra* note 34, at 352 (indicating subsection (a)(1) of the

through the spread of computer viruses or other programs.[129] The same frustrations accompanying the attempted prosecution of a Chinese citizen-hacker of a non-vital computer system would also, unfortunately, accompany any attempt to prosecute a Chinese citizen hacking a vital U.S. target.[130] It would be quite difficult to prosecute the hacker because of the absence of an extradition treaty with China.[131]

Even if there was an extradition treaty between the People's Republic of China and the United States in force, it is doubtful that an extradition would occur.[132] Most extradition treaties include a political offense exception,[133] which stipulates that a requested party will not grant extradition if the offense is considered a political offense or connected to a political offense.[134] China may view the actions of its citizen-hacker as a critique of the American capitalistic, democratic government and, therefore, consider it a political offense, absolving the Chinese government of any responsibility to extradite the citizen-hacker.[135]

If an attack caused considerable damage other than the mere shut down of a computer system, such as a plane crash resulting from a

---

CFAA as the subsection primarily regulating computer-related threats to national security).

129. *See* 18 U.S.C. § 1030(a)(5) (proscribing the "knowing . . . transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer"); *see also supra* notes 92-97 and accompanying text (discussing the provisions of the CFAA).

130. *See supra* notes 98-111 and accompanying text (discussing the resulting difficulties in attempting to bring a Chinese citizen before an American court).

131. *See id.* (commenting on the absence of an extradition treaty between China and the United States)

132. *See* Soma et al., *supra* note 34, at 353 (declaring that extraditions based on national security rarely occur because the infractions are usually considered political offenses and thus fall within the political offense exceptions that are written into the treaties).

133. *See* Greenberg et al., *supra* note 125.

134. *See* Soma et al., *supra* note 34, at 327 (describing the political offense exception, but also noting that a recent trend by European countries is to eliminate the exception because they view it as a defense for international terrorism and hate crimes).

135. *See id.* (discussing the implications of the political offense exception).

failure in the air-traffic control system, the United States could categorize the incident as a terrorist attack.[136] The international pressure to extradite a terrorist far exceeds any pressure to extradite common criminals.[137] This increased pressure is due in large part to the perception that the State refusing the extradition request sponsored or encouraged the terrorist act.[138] In this case, China will want to avoid implication because the complete refusal of a State to cooperate in the suppression or prevention of such hostile acts could be considered state-sponsorship of the action ipso facto.[139] This in turn would invoke the law of conflict management,[140] which authorizes the use of force in self-defense.[141] China and the United States, two nuclear powers, would then be exchanging hostilities on the dangerous brink of war.[142] Barring an agreement by the Chinese government to extradite the citizen-hacker, the United States is once again faced with very limited avenues of recourse for a debilitating computer attack on one of its vital computer systems when the attacker is a private citizen of China.[143]

---

136. *See* Robbat, *supra* note 45, at 14 (commenting on the international legal implications of computer-related terrorist attacks); *see also* Greenberg et al., *supra* note 125 (noting the international pressures and implied complacency associated with refusing an extradition request for the suspect of a terrorist act).

137. *See* Greenberg et al., *supra* note 125 (discussing the international pressures that coincide with an extradition request for a terrorist suspect).

138. *See* SHARP, *supra* note 67, at 8 n.14 (indicating that a failure to prevent or suppress a terrorist act could be perceived as sponsorship of that act, which could then implicate a self-defense response).

139. *See id.* (describing the possibility that state-sponsorship of a terrorist act constitutes a use of force by that State which could warrant a response of the use of force in self–defense).

140. *See id.* at 7 (defining the law of conflict management).

141. *See id.* at 8 n.14 (indicating that the law of conflict management permits the use of force in self-defense under certain circumstances and with certain limitations).

142. *See, e.g.*, Peter Baker, *Russia Seeks 5-Nation Talks On Reducing Nuclear Arms*, WASH. POST, July 7, 2001, at A19 (reporting that China and the United States both have nuclear weapons).

143. *See* Robbat, *supra* note 45, at 53 (declaring the current legal paradigm, regarding computer attacks originating on foreign soil, as "vague" and an insufficient deterrent in discouraging such computer attacks).

B. STATE-SPONSORED ATTACKS

1. Non-Vital Target

Recently, a computer worm called "Code Red" swept across the globe in two different waves.[144] The first wave infected nearly two hundred and eighty thousand computers, causing the Pentagon to temporarily block public access to its website, and the White House to change its numerical Internet address as a precautionary measure.[145] A second wave spread a new variant of the worm a week later and infected over one hundred and fifty thousand computers.[146] Among the second wave's victims were several of Microsoft's MSN Hotmail servers and the servers of the Associated Press.[147] The worm

144. *See* Nicole C. Wong, *'Code Red' Creeping Worldwide*, WASH. POST, Aug. 2, 2001, at E1 (reporting the spread of the second incarnation of the Code Red computer worm across the globe). Among its victims were the Pentagon, which had to install patches on many computers and had to take some websites offline to continue the work. *See id.* The worm traveled through the Internet by placing software code on unprotected business computers that then sent it to other machines that were typically the powerful server computers. *See id.* The worm itself also instructed other computers to flood certain websites with requests for data, overwhelming them and preventing legitimate users from accessing them. *See id.*

145. *See Pentagon Web Sites Blocked; Threat of 'Code Red' Computer 'Worm' Prompts Safeguards*, WASH. POST, July 24, 2001, at A5 [hereinafter *Pentagon Web Sites Blocked*] (describing the spread of the first Code Red virus that infected over two hundred eighty thousand computers and was the fastest spreading worm in history). Among the more high profile victims was the Pentagon, which temporarily blocked public access to its websites. *See id.* In addition, the White House was forced to change its Internet address as a precautionary move. *See id.*

146. *See* Wong, *supra* note 144, at E1 (describing the second incarnation of the Code Red worm).

147. *See* Nicole C. Wong, *Worm Sneaks Up on Firms Urging the Public to Download Fix*, WASH. POST, Aug. 10, 2001, at E2 (detailing the victims of "Code Red II"). In its second life, the Code Red virus infected many companies that had been urging the public to protect against it. *See id.* Microsoft Corp., which developed the software patch to protect against the worm, had some of its server computers infected by the bug. *See id.* The Associated Press, which had filed dozens of updates on the spread of the virus, was infected as well. *See id.* Many of those updates were delayed as the virus upset the timely posting of them to the organization's website. *See id.* In addition, many of the employees lost Internet access until the servers were repaired and went back online. *See id.*

defaced websites with the words "Hacked by Chinese."[148]

Although no one has taken credit for the "Code Red" attack,[149] if a private citizen is responsible for the hack, then the incident is a law enforcement issue with international implications.[150] If, however, the Chinese government was the perpetrator, the incident would be governed by the international laws controlling the relationships between States.[151] The imposition of these international laws avoids many of the extradition obstacles that hamper any legal pursuit by the United States of a Chinese citizen-hacker.[152] Unfortunately, the responses available to the United States remain unclear because of the ambiguity of the applicable international laws that apply to computer attacks.[153]

In the hypothetical scenario, envisioning the Chinese government as the perpetrator of the "Code Red" attack, since damage was intentionally inflicted by one sovereign nation within the territorial boundaries of another nation, the international law of conflict management is implicated.[154] As such, the United States' response would be dictated by the provisions of the United Nations Charter ("U.N. Charter"), which defines and governs the use of force, both

148. *See Pentagon Web Sites Blocked*, *supra* note 145, at A5 (describing the damage caused by the worm).

149. *See* Wong, *supra* note 144, at E1 (reporting a lack of indication regarding the worm's origin).

150. *See* SHARP, *supra* note 67, at 8 n.14 (arguing that all "hostile, transnational activities in CyberSpace" are either independent of state-sponsorship and thus a crime to be addressed by national and peacetime treaty law, or state-sponsored and thus a use of force governed by the law of conflict management and the law of armed conflict). Of course, even if state-sponsorship were proven, the actual hacker could still be tried under the criminal laws, if he could be extradited. *See supra* notes 88-119 and accompanying text.

151. *See* SHARP, *supra* note 67, at 8 n.14 (indicating that the involvement of a nation-state implicates international laws governing relations between States).

152. *See supra* notes 98-110 and accompanying text (discussing the near impossibility of bringing a Chinese citizen to justice in the United States because of the lack of an extradition treaty between the two countries).

153. *See* Robbat, *supra* note 45, at 32 (noting that the legality of any particular response to a computer attack is unclear under the current international law framework provided by the U.N. Charter and other treaty law).

154. *See* SHARP, *supra* note 67, at 7 (declaring the law of conflict management to govern the use of force during peacetime).

during peacetime and armed conflict.[155] Article 2(4) of the U.N. Charter prohibits the threat or use of force against the territorial integrity of another nation,[156] unless it is conducted pursuant to a nation's right to self-defense or authorized by the U.N. Security Council.[157] In addition, the prohibition on the use of force encompasses both military and non-military force, in an acknowledgment that non-military force can cause the same damage and destruction as conventional military force.[158] Therefore, China's state-sponsored computer attack, so long as it intentionally causes damage, would most likely be considered a use of force prohibited by Article 2(4) of the U.N. Charter.[159]

Although the perpetrator, rather than the target or amount of damages, dictates the controlling law—national and treaty law for

---

155. *See id.* at 6-7 (discussing the relationship between the peacetime regime of international law, the law of conflict management, and the law of armed conflict).

156. *See* U.N. CHARTER art. 2, para. 4 (proclaiming "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations"); *see also* SHARP, *supra* note 67, at 33 (explaining the Article 2(4) prohibition on the use of force).

157. *See* SHARP, *supra* note 67, at 34 (declaring that any State's use of force is unlawful under Article 2(4) of the U.N. Charter unless that action is an exercise of the State's inherent right of self-defense, as codified in Article 51 of the U.N. Charter, or is authorized by the Security Council "under its coercive Chapter VII authority"). Article 51 states:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

U.N. CHARTER art. 51.

158. *See* SHARP, *supra* note 67, at 101 (declaring that the use of force prohibition covers "'physical force of a non-military nature' committed by any state agency") (quoting BRUNO SIMMA, THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 113 (1994)).

159. *See id.* at 101-02 (demonstrating how a state activity in cyberspace that intentionally causes *any* destructive effect within the sovereign territory of another State is an unlawful use of force within the meaning of Article 2(4)).

private citizens or the international law of conflict management for states[160]—the opposite is true in measuring an appropriate response.[161] A response to the use of force by a State is generally controlled by the severity of the initial use of force.[162] In the case of a cyber-attack on a non-vital U.S. target that causes minimal physical destruction, the attack will most likely be considered an illegal use of force.[163]

The scope, duration, and intensity of such a cyber-attack, however, would not be sufficient to qualify it as an armed attack.[164] If the attack is not considered an armed attack, then it is doubtful that the use of force would be authorized under the United States' right to self-defense,[165] because the right to respond in self-defense is predicated on an armed attack.[166] In addition, a state's right to use force in self-defense is controlled by the principles of necessity[167]

---

160. *See id.* at 8 n.14 (noting that all types of cyber-attacks, regardless of the target, are either non-state-sponsored, and thus a criminal matter to be resolved through national and peacetime international treaty law, or state-sponsored and controlled by the international law of conflict management and the law of armed conflict).

161. *See id.* at 103 (stating that even if the intentional destructive action is considered a use of force, it may not contain the intensity or severity to be considered an armed attack deserving of a corresponding use of force in self-defense).

162. *See id.* (noting that the intensity and severity of the initial attack determines the appropriate response in terms of whether to use force and if so, how much).

163. *See id.* (positing that any action by one nation that intentionally causes damage in another is an unlawful use of force).

164. *See* SHARP, *supra* note 67, at 55-67 (describing the threshold point of an armed attack at which the use of force is justified as an exercise of a State's inherent right to self-defense in terms of scope, duration, and intensity).

165. *See id.* at 103 (noting that response to an incident that causes minimal damage and does not constitute a continuing threat may very well be considered an unlawful use of force, but does not qualify as an armed attack, and thus does not implicate a victim State's right to use force as self-defense).

166. *See* Schmitt, *supra* note 32, at 920 (arguing that an armed attack and not just the use of force is what triggers a State's right to respond with force in self-defense).

167. *See* SHARP, *supra* note 67, at 38 (stating that the law of conflict management requires that a State's use of force be necessary for its self-defense).

and proportionality,[168] among others, and is prohibited for retaliatory or punitive purposes.[169]

A response in kind by the United States, such as the release of a similar virus in China, could be viewed as a retaliatory or punitive use of force.[170] Such an attack would be prohibited by international law because it would not be in response to the equivalent of an armed attack.[171] The United States could appeal to the U.N. Security Council, which is authorized under Article 39 of its Charter,[172] to respond with force to any event that threatens peace, even if the event does not meet the threshold of an armed attack.[173] Barring

---

168. *See id.* (requiring "that a State's use of force be proportional in intensity and magnitude to what is reasonably necessary to promptly secure the permissible objectives of self-defense.").

169. *See id.* at 37-39 (discussing the principles that control a State's use of force in self-defense).

170. *See id.* (stating that customary international law prohibits the use of force for retaliatory or punitive actions).

171. *See supra* notes 160-169 and accompanying text (illustrating the parameters within which a responsive use of force may take place).

172. *See* U.N. CHARTER art. 39 (stating "[t]he Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security"). Articles 41 and 42 describe the sanctions available to the Security Council to maintain or restore peace and security, which include complete or partial interruption of economic or diplomatic relations and military actions. *See* U.N. CHARTER arts. 41 and 42. The United States and China are both permanent members of the Security Council and thus have vetoes over any action the Security Council takes. *See* SYDNEY D. BAILEY, THE PROCEDURE OF THE U.N. SECURITY COUNCIL 107 (2d ed. 1998). Because both countries would be parties to the dispute for which the proposal for pacific settlement would be offered, they would be required to abstain from voting as set forth in Articles 27(3) and 52(3) of the Charter. *See id.* at 224. Article 27(3) states that "[d]ecisions of the Security Council on all other matters shall be made by an affirmative vote of nine members including the concurring votes of the permanent members; provided that, in decisions under Chapter VI, and under paragraph 3 of Article 52, a party to a dispute shall abstain from voting." U.N. CHARTER art. 27(3). Article 52(3) states that "[t]he Security Council shall encourage the development of pacific settlement of local disputes through such regional arrangements or by such regional agencies either on the initiative of the states concerned or by reference from the Security Council." U.N. CHARTER art. 52(3).

173. *See* Schmitt, *supra* note 32, at 920 (noting that a determination that a specific act does not constitute an armed attack to which a responsive use of force

action from the Security Council, the United States' official unilateral responses are limited.[174] If early detection and other preventive measures[175] fail, the United States may be able to ask for reparations for any damage done as well as publicly disclose the Chinese government's role in the computer attack to cause international embarrassment.[176] Ultimately, the legality of any action the United States takes is questionable because there are no current laws or international agreements, especially between the United States and China, which deal explicitly with this type of computer attack.[177]

---

is justified does not leave the international community remediless). Thus, a State victimized by an isolated attack that does not amount to an armed attack could not respond to it with force on its own accord, but if the Security Council determined the act to be a sufficient threat or potential threat to international peace and security, then the Security Council could authorize a response. *See id.* at 929.

174. *See supra* notes 144-173 (analyzing the remedies the United States has as a State in response to an attack by China). Private citizens could, of course, exact their own revenge by unleashing a virus in China or hacking into the computers of Chinese citizens or the Chinese government and be relatively free of prosecution. *See supra* notes 88-119 and accompanying text (discussing the paucity of remedies available to a U.S. victim of a Chinese hack). For the same reason that U.S. citizens are largely remediless if victimized by a Chinese hacker, so too would a Chinese citizen be largely remediless if victimized by a U.S. hacker. *See id.*

175. *See* SHARP, *supra* note 67, at 130 (describing the appropriate remedies to the unlawful use of force in the form of a computer attack that falls short of justifying a use of force response).

176. *See id.* at 130 (proposing public disclosure and subsequent embarrassment to the offending State as appropriate responses to computer attacks that do not pose instant and overwhelming need for anticipatory self-defense); *see also* Schmitt, *supra* note 32, at 290 (declaring that a computer attack that falls short of an armed attack but nonetheless violates the Article 2(4) prohibition on the use of force would subjugate the offending State to "international opprobrium"). It is important to note that these responses, especially the public disclosure for embarrassment purposes, are theoretical and focus on what international law permits. *See supra* notes 45-63 and accompanying text. This Comment focuses on the available legal responses and not whether these responses are good policy. *See id.* Actual responses to a computer attack originating from China would obviously need to be determined in the much broader context of U.S. foreign policy and the already complex and difficult relationship between the two countries. *See id.*

177. *See* Bowman, *supra* note 25, at 1945 (discussing the agreement by the G-7 Ministerial Conference to find solutions to the computer attack problem, which falls far short of any binding or controlling law).

2. Vital Target

Hoping to put the skills of its amateur hackers to use, China's People's Liberation Army recently began recruiting civilian hackers and training them as "cyber warriors" at military schools.[178] In fact, China places such emphasis on the ability to wage Information Warfare[179] it is openly contemplating the development of a fourth branch of its armed services dedicated to IW.[180] The United States is also beginning to focus on IW.[181] Military computer technicians employed by the United States Defense Information Systems Agency are being trained to defend against hostile computer attacks from other countries, as well as launch their own attack against an adversary's computer systems.[182] As a policy tool, computer attacks on vital national infrastructure targets might be as effective, if not

178. *See* Cilluffo et al., *supra* note 30, at 151 (describing a call in the *Liberation Army Daily*, the official newspaper of the People's Liberation Army, to recruit civilian hackers in order to facilitate the ability to wage war over the Internet).

179. *See* Robbat, *supra* note 45, at 5 (defining "Information Warfare" as the "employment of computers and related technology to attack computer networks linked to a nation's civilian, military, and/or government information-based resources."). This is a narrower definition for IW than the frequently cited Air Force definition, which characterizes IW as "[a]ny action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions." Ronald R. Fogleman & Sheila E. Windnall, *Cornerstones of Information Warfare*, U.S. DEPARTMENT OF THE AIR FORCE, *available at* http://www.af.mil/lib/corner.html (last visited Nov. 7, 2001)

180. *See* Bill Gertz, *China Plots Winning Role in Cyberspace: Military Paper Cites Need for 'Paralyzing' Internet Software*, WASH. TIMES, Nov. 17, 1999, at A1 (noting that the *Liberation Army Daily*, the official newspaper of the People's Liberation Army, contained an article calling for the establishment of a "net force" as an additional military branch).

181. *See* Andrea Stone, *Cyberspace is the Next Battlefield: U.S., Foreign Forces Prepare for Conflict Unlike Any Before*, USA TODAY, June 19, 2001, at 1A (reporting on the United States' involvement in IW plans).

182. *See id.* (commenting on the emergence of cyberwarfare as one of the most significant national security threats and discussing measures the United States has taken to protect against it). In addition, Pentagon officials have commented on the vast computer warfare arsenal they have developed. *See id.* Although officials will not comment on what comprises this arsenal, most analysts agree that it probably includes various computer viruses, logic bombs, worms and Trojan horses. *See id.* Officials are most concerned with the ability to focus attacks on strategic targets in order to avoid civilian casualties in the event an attack actually occurs. *See id.*

more effective, than conventional attacks.[183] In fact, many predict the next international conflict between two technologically advanced countries will involve computer attacks.[184]

As noted earlier, once it is determined that a State, or state agent, is responsible for an action that causes damage in the territory of the victim State, the victim's response is controlled by international law of conflict management and the law of armed conflict.[185] In the case where the state-sponsored attack is directed against a vital computer system,[186] the damage is likely to be of such magnitude so as to qualify the attack as a use of armed force.[187] This then triggers the victim State's right to respond with force in self-defense under Article 51 of the U.N. Charter.[188] The response must, of course,

---

183. *See id.* at 2A (reporting that some countries, recognizing their inferior military strength to the United States, view IW as an alternative approach that could level the playing field). As such, Secretary of Defense Donald Rumsfeld ranks IW as one of the gravest threats to national security. *See* Stone, *supra* note 181, at 2A; *see also* Robbat, *supra* note 45, at 9 (discussing the appeal IW holds to smaller nations as a means to overcome battlefield inferiority).

184. *See* Stone, *supra* note 181, at 2A (quoting Dan Kuehl, a teacher of Information Warfare at the National Defense University who predicts "[t]he next time you see a major conflict between two technologically advanced opponents, you're going to see computer network attacks"). In fact, U.S. officials admit to already having used computer attacks. *See id.* During the Gulf War, U.S. warplanes emitted jamming signals that interfered with the Iraqi air-defense computers' ability to target allied aircraft. *See id.* In addition, during the war in Kosovo in 1999, U.S. officials considered electronically siphoning the bank accounts of Serbian President Slobodan Milosevic. *See id.* They opted not to out of concerns for the legality of the operation. *See id.*

185. *See supra* notes 161-169 and accompanying text (indicating that any response to an attack orchestrated by a State is controlled by international law of conflict management and the law of armed conflict).

186. *See supra* notes 77-78 and accompanying text (delineating what the United States considers to be its vital infrastructures and computer systems).

187. *See* SHARP, *supra* note 67, at 138 (indicating that when "an activity not traditionally considered an armed attack is used in such a way that it becomes tantamount in effect to an armed attack," it will generally be considered an armed attack).

188. *See id.* at 36 (setting forth that Article 51 of the U.N. Charter recognizes the right of all nations to defend against unlawful, aggressive use of force); *see also id.* at 130 (stating that when a threat to a vital national interest, such as the one posed by a computer attack on the computers that maintain the safety and reliability of the nuclear stockpile, is detected, the victim State is legally permitted to respond with necessary and proportional force in an act of anticipatory self-defense).

comply with the principles of necessity and proportionality, but can be in the form of traditional military force, or a response in kind.[189] Although a response in kind, or even a response through traditional military capabilities may be legal,[190] it means that the world's two most powerful nations are exchanging hostilities.[191]

The available legal responses to full-scale computer attacks by one nation against another are still somewhat ambiguous, but are nonetheless broadly controlled by the U.N. Charter.[192] Even if clarified, the controlling laws are merely placing parameters on the conduct of war.[193] The restrictions on, and deterrence of, an initial attack should be clarified in order to avoid a subsequent response.[194]

III. RECOMMENDATIONS

A. ADDRESSING THE VULNERABILITIES

One of the easiest ways to avoid the ambiguities and difficulties surrounding the available legal responses to computer attacks is to

---

189. *See id.* at 38 (discussing the principles of necessity and proportionality, as well as noting that any self-defense response is prohibited from being retaliatory or punitive).

190. *See supra* notes 156-189 and accompanying text (setting forth the legality of a use of force by one nation as a self-defense response to a use of force by another nation).

191. *See* Richard Bernstein & Ross Munro, *The Coming Conflict with America*, FOREIGN AFF. Mar./Apr. 1997, 18, 21-22 (describing China as rapidly becoming the globe's second most powerful nation and the next chief rival to the United States).

192. *See* SHARP, *supra* note 67, at 33 (indicating the U.N. Charter clearly outlaws the aggressive use of force).

193. *See* Robbat, *supra* note 45, at 53 (indicating the absence of any deterrent force to the use of IW in international law).

194. *Compare supra* notes 170-177 and accompanying text (analyzing the responses available to the United States in the case of a computer attack on a non-vital target with a request for economic reparations being the most severe), *with supra* notes 186-191 and accompanying text (describing the most severe response to a computer attack on a vital target as culminating in a war between the two most powerful nations in the world). *See also* Robbat, *supra* note 45, at 53 (arguing that the current international legal paradigm lacks sufficient deterrents to discourage debilitating computer attacks).

avoid the need to respond altogether.[195] Adequate protective measures, as well as deterrent measures,[196] negate the need to respond because they prevent an attack from causing any damage in the first place.[197] Thus, the United States should first address its vulnerabilities to hacks of any kind.[198]

To protect the nation's vital computer systems, the United States must recognize computer attacks as emerging threats on the same level as terrorism and weapons of mass destruction.[199] The U.S. government should direct appropriate resources to preventing computer attacks.[200] Appropriately, President Clinton signed Presidential Decision Directive 62 ("PDD-62")[201] and Presidential

---

195. *See* discussion *infra* notes 198-200 and accompanying text (discussing the benefits of protective and deterrent measures).

196. *See* Col. James P. Terry, USMC (Ret), *Responding to Attacks On Critical Computer Infrastructure: What Targets? What Rules of Engagement?*, 26 NAVAL, L. REV. 170, 184 (1999) (noting that the importance of recognizing cyber-terrorism as a strategy that does not follow any traditional military patterns is the realization that deterrence is thus the only credible response).

197. *See, e.g.*, Wong, *supra* note 144, at E1 (describing a patch issued by Microsoft to protect computers from the Code Red worm). More than a million users downloaded the patch. *See id.* As such, no customer lost any data. *See id.*

198. *See, e.g.*, *supra* note 193-194 and accompanying text (stressing the need to emphasize deterrence).

199. *See Security in Cyberspace: Hearings Before the Permanent Subcomm. on Investigations of the S. Comm on Gov't Aff.*, 104th Cong. 5 (1996) (prepared statement of Sen. William V. Roth, Jr., Chairman) (indicating that the protection of the county's computer networks should be of vital concern).

200. *See* Thomas E. Ricks, *Rumsfeld Mulls Two Options: Status Quo or 10% Military Cut*, WASH. POST, Aug. 9, 2001, at A4 (identifying computer attacks, along with terrorism and the proliferation of missiles in the Third World, as the preeminent emerging threats to be addressed by the new military strategy being devised by Secretary of Defense Rumsfeld). The Secretary's recently released military strategy for the Twenty-First Century, entitled "Terms of Reference," calls for new computer warfare abilities and places defense against computer attacks and computer warfare as one of the military's primary functions. *See id.* In addition, the Pentagon has asked for a five hundred percent increase in funding for the Defense Information Systems Agency, from $3.1 million to $18.6 million in 2002, in order to better guard the military's 2.5 million computers. *See also* Stone, *supra* note 181.

201. *See* The White House, Office of the Press Secretary, Fact Sheet on Presidential Decision Directive 62, (May 22, 1998) [hereinafter Fact Sheet on PDD-62] (announcing the signing of PDD-62, which creates the Office of the National Coordinator for Security, Infrastructure Protection, and Counter-

Decision Directive 63 ("PDD-63")[202] in May of 1998 in an effort to implement the recommendations of the PCCIP Report.[203] These two directives collectively form the foundation of the government's efforts to protect the country's vital infrastructures.[204] The directives created the Office of Coordinator for Security, Infrastructure Protection, and Counter-Terrorism[205] and the National Infrastructure Protection Center ("NIPC") at the FBI.[206] This is a collaborative effort between government agencies and the private sector to combat the threat of computer attacks on vital U.S. computer systems.[207] It is thus important to ensure that this initiative remains a top priority and is allocated the appropriate resources to ensure its ability to respond to the growing number of threats against the United States's vital computer systems.[208]

Terrorism), *available at* http://www.fas.org/irp/offdocs/pdd-62.htm (last visited Sept. 18, 2001).

202. *See* The White House, Office of the Press Secretary, Fact Sheet on Presidential Decision Directive 63, (May 22, 1998) [hereinafter Fact Sheet on PDD-63] (specifying the Administration's broad policy outlined in PDD-62 and creating the National Infrastructure Protection Center (NIPC) at the Federal Bureau of Investigation ("FBI")), *available at* http://www.fas.org/irp/offdocs/pdd-63.htm (last visited Sept. 18, 2001). The NIPC incorporates representatives from the FBI, the Departments of Defense, Energy, and Transportation, the United States Secret Service, and the Intelligence Community, as well as the private sector, to coordinate the Federal Government's actions with regard to threats on the National Infrastructure. *See id.*

203. *See* Persico, *supra* note 78, at 165-66 (analyzing PDD-62 and PDD-63).

204. *See id.* at 166 (stating that PDD-62 and PDD-63 form the foundation of the government's endeavor to protect the vital infrastructures).

205. *See supra* note 201 (announcing the creation of the Office of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism through the signing of PDD-62).

206. *See supra* note 202 (indicating the creation of the National Infrastructure Protection Center ("NIPC") at the FBI through the signing of PDD-63).

207. *See* Persico, *supra* note 78, at 166 (discussing the purposes of PDD-62 and -63); *see also Cyber-attacks: The National Protection Plan and its Privacy Implications: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the S. Comm. on the Judiciary*, 106th Cong. 20 (2000) (statement of John S. Tritak, Director, Critical Infrastructure Assurance Office) (elaborating on the government's progress in implementing the National Plan set forth in PDD-63).

208. *See Cyber-attack: Improving Prevention and Prosecution: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the S. Comm. on the Judiciary*, 106th Cong. 68-69 (2000) (statement of Guadalupe

Furthermore, network administrators for non-vital computer systems would greatly benefit from attending a seminar on protecting computer networks from attack.[209] Some of these seminars are run by major U.S. corporations such as Ernst and Young and are offered in growing numbers.[210]

B. INTERNATIONAL AGREEMENTS

1. The Lone Hacker

If the preventive measures prove inadequate and a computer attack occurs, the current legal framework is inadequate to respond.[211] The lack of an agreement with China, whether a bilateral extradition treaty or a multilateral international agreement, prevents an action to seek legal redress from a lone Chinese citizen-hacker, regardless of the importance of the victimized computer system.[212] Similarly, the lack of any international agreement explicitly addressing computer

---

Gonzalez, Special Agent In Charge of the FBI's Phoenix Field Office) (testifying that the NIPC needs more than double the current number of field investigative personnel but that the program was not, at the time, slated for any budgetary increases).

209. *Compare* Kevin McCoy, *Execs Become Hackers to Learn How to Stop Snoopers*, USA TODAY, June 19, 2001, at 6B (reporting on the growing number of seminars aimed at teaching defensive skills to protect computer networks from hackers), *with infra* notes 200-208 and accompanying text (discussing steps the government is taking to protect its computer systems, as well as those private industry systems included in any of the vital national infrastructures). Many corporations are now spending upwards of five thousand dollars per person to send their top computer executives to these types of seminars. *See* McCoy, *supra*, at 6B. The seminars are generally five days long and consist of nine hour days dedicated to hacking. *See id.* In the hopes of learning the skills needed to protect their company's computer systems, the students try to hack into a computer network created by the instructors for this very purpose. *See id.* As one instructor noted, "it helps if you think like your opponents and try to anticipate what they might do." *Id.*

210. *See* McKoy, *supra* note 209, at 6B (describing the hacker prevention seminars).

211. *See* discussion *supra* Part II (discussing the difficulties the United States would have in pursuing a legal course of action in response to a computer attack originating in China).

212. *See* discussion *supra* Part II (A) (discussing the available remedies to a computer attack on both a vital and non-vital computer network from a private Chinese citizen).

attacks between nations creates an equally ambiguous legal course of action for any victim nation.[213]

The United States could enter into a mutual prosecution agreement with China in order to facilitate the prosecution of, and possibly secure the potential for economic damages from, a private Chinese citizen who hacks into and damages either a vital or non-vital U.S. computer system.[214] Such an agreement would be a pledge by both countries to bring to justice, through their own judicial system, hackers that cause damage in the other's country, as opposed to a mutual legal assistance treaty[215] into which the United States would be unwilling to enter with China.[216]

Ideally, the international community will come to some sort of agreement on computer attacks and crimes.[217] Both the United States and China would benefit more from a multilateral agreement rather than a bilateral agreement.[218] A multilateral agreement would be a greater deterrent and a more reliable framework for seeking damages.[219] It would protect both the United States and China from

---

213. *See* discussion *supra* Part II (B) (examining the inadequacy of the current international legal framework in addressing computer attacks by one country against another).

214. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES: INTERNATIONAL AGREEMENTS: DEFINITION, NATURE AND SCOPE § 302 reporter's notes 2 (1987) (stating that "there is no principle either in international law or in United States constitutional law that some subjects are intrinsically 'domestic' and hence impermissible subjects for an international agreement"). Thus, there is nothing preventing the two countries from legally coming to some sort of cooperative agreement, given the unlikelihood of the two countries ever agreeing to an outright extradition treaty. *See supra* note 101.

215. *See, e.g.*, Treaty with Russia on Mutual Legal Assistance in Criminal Matters, June 17, 1999, U.S.-Russ., S. TREATY DOC. NO. 106-22 (binding the two countries into a mutual legal assistance treaty which involves mutual cooperation on such procedures as service of process, extradition, and criminal investigation).

216. *See* HENKIN, *supra* note 101, at 270 (indicating that the United States does not enter into treaties of any sort with countries it considers repressive).

217. *See* Soma et al., *supra* note 34, at 363 (arguing for a convention relating to the extradition of computer criminals).

218. *See infra* notes 219-221 and accompanying text (discussing the benefits of a multilateral agreement over a bilateral agreement).

219. *But see* Senator Jesse Helms, Floor Statement (Apr. 26, 2000) [hereinafter Statement of Jesse Helms] (expressing America's reluctance to enter into agreements that do not bind the countries about whom America is most worried by

computer attacks originating anywhere in the globe, rather than only from each other.[220] The agreement will also serve as another vehicle for China's increased participation in the international community.[221]

The two most promising incarnations of such an agreement take the forms of a multilateral extradition agreement[222] and the creation of a neutral arbitration body.[223] A multilateral extradition agreement would bind all signatories under one broad framework of extradition law.[224] This serves to provide uniform extradition requirements and an agreement on extraditable crimes.[225]

Alternatively, the United States and China could, along with the rest of the international community, agree to submit to the jurisdiction of a neutral arbitration body, such as the International Court of Justice[226] or the International Criminal Court.[227] This would

---

stating that any treaty then President Clinton negotiated with Russia regarding the Anti-Ballistic Missile Treaty would be "dead on arrival" because of threats from China, Iraq, and North Korea, who were not signatories).

220. *See, e.g., infra* note 224 and accompanying text (indicating the broad, binding authority a multilateral agreement could have on a large number of signatories).

221. *See* Robert S. Ross, *Beijing as a Conservative Power*, FOREIGN AFF., Mar. 13, 1997, 33, 41 (listing the various international organizations into which the United States should invite China, thus indicating China's relative lack of involvement in international organizations).

222. *See infra* notes 224-225 and accompanying text (discussing a multilateral extradition agreement).

223. *See infra* notes 226-228 and accompanying text (presenting the issues associated with the creation of, and submission to, a neutral international arbitration body).

224. *See* Soma et al., *supra* note 34, at 363 (arguing for a convention relating to the extradition of computer criminals).

225. *See id.* at 363-64 (elaborating on the specifics of a proposed multilateral extradition agreement). Although the convention would involve numerous countries, the United States may still be reluctant to agree to terms that would turn its citizens over to repressive governments. *See* HENKIN, *supra* note 101, at 270 (noting the United States does not enter into extradition treaties with countries it considers repressive).

226. *See* Perritt, *supra* note 106, at 106 (indicating that some scholars suggest expanding the role of the International Court of Justice to include jurisdiction over international crimes).

227. *See id.* at 106-07 (proposing the International Criminal Court as an appropriate venue for international computer crime cases).

provide uniformity in the treatment of transnational computer crimes and ensure that no crime goes unpunished.[228] Admittedly, such agreements are rather idealistic,[229] and it may, unfortunately, take a devastating cyber-event to spur the international community into adopting such sweeping pro-active measures.[230]

2. Controlling State Actions

Many of the same difficulties associated with reaching an international agreement or understanding on the treatment of cyber-crimes perpetrated by private citizens are also present in any discussion concerning the hostile use of computers by states.[231] A bilateral agreement with China condemning the use of computer attacks would only protect the United States and China from attacks by each other. However, this would not protect either country from the rest of the world.[232] Thus, if either country enters into an international agreement, that agreement needs to include as many nations as possible.[233]

In order to avoid many of the difficulties associated with the negotiation of a new international agreement,[234] the United States and China could work together to clarify an already existing agreement—

---

228. *But see id.* at 224-28 (presenting the numerous difficulties associated with the creation of an international arbitration body for cyber-crimes, not the least of which is the absence of uniformity of standards for the treatment of cyber-crimes). If nothing else, an international agreement of this sort could better deter the hacker who would have to conceal his actions from the combined signatories' investigatory powers, rather than just one or two countries. *See id.*

229. *See, e.g.*, Statement of Jesse Helms, *supra* note 219 (demonstrating the difficulty in reaching binding, multilateral agreements on difficult issues).

230. *See* Cilluffo et al., *supra* note 30, at 136-37 (lamenting the fact that it is a tenet of human nature to believe that which has not happened cannot happen).

231. *See supra* notes 224-230 and accompanying text (assessing the complexities in reaching an international agreement on cyber-crimes).

232. *See* Robbat, *supra* note 45, at 9 (dubbing IW "the great equalizer" for smaller nations attacking adversaries with superior conventional military capabilities).

233. *See supra* note 219 (using the failure of the Anti-Ballistic Missile Treaty to demonstrate the necessity of binding as many nations as possible to such an agreement in order to gain ratification of the agreement).

234. *See supra* notes 217-233 and accompanying text (indicating the difficulties associated in creating binding international agreements).

the U.N. Charter.[235] The U.N. could definitively declare computer attacks as an armed use of force prohibited by Article 2(4) of the U.N. Charter.[236] This erases some ambiguity surrounding the issue and is not difficult to accomplish, because it does not involve the creation of any new organizations.[237] In addition, it clarifies the course of action the victim nation can take in accordance with international law.[238]

While this clarification may deter states from conducting computer warfare,[239] the certainty of the response hopefully serves as the ultimate deterrent.[240] Somewhat similar to the mutual assured destruction theory of preventing nuclear war, a clear policy that computer attacks are met with the severest responses, both conventionally and electronically, serves to outweigh potential benefits that arise from instigating the initial computer attack.[241]

CONCLUSION

The increased growth of, and dependence on, the Internet revolutionized the transfer of information.[242] At the same time, it

---

235. *See infra* notes 236-238 and accompanying text (presenting the possibility of unequivocally including cyber-attacks within the meaning of Article 2(4)'s prohibited use of force in the U.N. Charter).

236. *See* Morth, *supra* note 27, at 590 (arguing that the use of the IW should be considered a use of force prohibited by Article 2(4) of the U.N. Charter); *see also* Robbat, *supra* note 45, at 56 (proposing the U.N. agree that IW invokes Article (2)4 as well as Article 51 of the U.N. Charter).

237. *See supra* note 217-233 and accompanying text (discussing the challenges inherent in the creation of binding international agreements and international bodies).

238. *See* Robbat, *supra* note 45, at 55 (stating that IW currently circumvents international law because of definitional ambiguity, rather than a lack of relevant provisions).

239. *See* Morth, *supra* note 27, at 588 (arguing that Article 2(4) impacts the conduct of states, thereby refuting the proposition that international law is largely ignored due to the absence of any coercive power).

240. *See* Robbat, *supra* note 45, at 62 (stating that any new legal paradigm designed to prevent the use of IW will only succeed if it contains sufficient repercussions that outweigh any potential benefits of conducting the IW).

241. *See id.* (noting that a lack of accountability will "encourage increased and reckless use of IW").

242. *See* Bowman, *supra* note 25, at 1937 (asserting that the National

added another tool to the vast arsenal of instruments available for criminals to pursue their nefarious deeds.[243] In addition, computer use in criminal activities significantly complicates the law enforcement agent's task of identifying criminals and especially apprehending them.[244] This is especially true when the search is international.[245] In the hands of a technologically advanced military, the Internet becomes a new weapon, potentially as powerful and disruptive as a nuclear explosion.[246]

Since the United States is one of the most technologically advanced nations,[247] it is also one of the nations most vulnerable to an incapacitating attack on its information infrastructure.[248] Nonetheless, the current legal structure is ill-suited to provide adequate remedies to a victim of a computer attack that originates outside the borders of the victim's country, regardless of the severity of the attack, the identity of the victim, or even the identity of the perpetrator.[249] The same American computer systems that are

---

Information Infrastructure, including the Internet, gives the average citizen a means of global access and personal participation rivaled only by the town meeting).

243. *See, e.g.*, Katyal, *supra* note 82 (discussing the plethora of computer related crimes including unauthorized disruption and identity theft, as well as traditional crimes using a computer, such as child pornography, copyright infringement, cyberstalking, and illegal firearms sales).

244. *See id.* at 1071-72 (describing the many difficulties encountered in attempting to identify a computer hacker).

245. *See id.* (discussing the problems associated with identifying a hacker); *see also* Perritt, *supra* note 106, at 2-3 (analyzing the jurisdictional, venue, and choice of law difficulties found in investigating and prosecuting computer crimes, as illustrated by the situation where a person in Mexico writes a defamatory message about a Norwegian that is read by someone in Israel through a U.S. server).

246. *See* Strobel et al., *supra* note 27, at 32 (equating the potential destruction of a debilitating computer attack to a nuclear explosion).

247. *See* Robbat, *supra* note 45, at 14 (commenting on the United States' heightened vulnerability to computer attacks). The United States' status as one of the most technologically advanced nations also means that it is one of the nations most dependent on information technology. *See id.*

248. *See id.* (delineating the seriousness of the threat of a cyber-attack on the United States).

249. *See* discussion *supra* Part II (analyzing the legal responses available to the United States in the event of a computer attack from any system originating in China).

vulnerable to a coordinated military computer attack are just as vulnerable to a lone hacker.[250] The available responses to each type of attack are equally ambiguous, especially if the attack originates from China.[251]

The United States must make concerted efforts to address its vulnerabilities and protect its computer systems from damaging attacks.[252] An attack repelled by a defense mechanism already in place negates the need to respond at all.[253] Therefore, adequate resources must be provided for this defensive effort, as well as training with the most up-to date information to keep abreast of the rapidly evolving hacker world.[254] If an attack happens to penetrate the initial defenses, there must be multilateral international agreements in place that explicitly detail the potential course of action for victim nations if the attack was instigated by another country.[255] Similarly, there must be codified multilateral international agreements providing for the prosecution of a computer hacker who perpetrates an attack against another country.[256] The Internet's blurring of international lines makes the need for international cooperation that much more critical, if, for no other reason than pure self-preservation, now that any nation can be brought to its knees with the single click of a mouse.

---

250. *See* Stone, *supra* note 181, at 1A (noting that computer technicians for the Defense Information System Agency are protecting defense computers from foreign countries as well as hackers).

251. *See* discussion *supra* Part II (analyzing the legal responses available to the United States in the event of a computer attack originating in China on any U.S. computer).

252. *See supra* notes 197-200 and accompanying text (discussing the need for preventive measures to secure the country's computer systems against attacks).

253. *See id.* (describing various protective measures).

254. *See id.* (citing the resources needed to protect computer systems).

255. *See* Morth, *supra* note 27, at 590 (arguing that IW should be considered a use of force prohibited by Article 2(4) of the U.N. Charter); *see also* Robbat, *supra* note 45, at 56 (proposing the U.N. agree that IW invokes Article (2)4 as well as Article 51 of the U.N. Charter).

256. *See supra* notes 214-228 and accompanying text (discussing the need for a multilateral international agreement on the prosecution of hackers).