And it appears that these new perspectives could be re-thought and explored by using the language of human rights.

In 2000, addressing a special session of the United Nations General Assembly, U.S. State Secretary Madeleine Albright said that "we must also learn more about the positive and negative impacts of globalization and trade on the lives of women. Because we don't know as much as we should and, unless we learn more, we will not be doing as much as we should to ensure that trade works for all people."[171]

Indeed, for so long now, politicians—even diplomats—and governments have used the right to development, gender equality and children's rights as political slogans. And the challenge today is for governments and nations—as indicated to us by Secretary Albright—to be able to look beyond the politics and economics of female migration as a distinct Third-World development phenomenon, and really explore the possibility of integrating human rights discourse in, and human rights-based approaches, to development. There is a need to integrate economic efficiency, therefore, with broader social objectives and considerations.[172] For only then can we truly claim that the development we have come to embrace is the type that fulfils the aspirations of developing nations to attain the greatest possible freedom and dignity as human beings.

171. Albright Address, *supra* note 106. Secretary Albright also quoted former First Lady Hillary Clinton that "when it comes to women, globalization should not mean marginalization." *Id.*

172. United Nations Center for Human Rights, *Realization of the Right to Development*, HR/PUB/91/2 (1991), at ¶ 67.

Cyberattacks, Cyberterrorism and Cyber-use of Force: Countering the Unconventional under International Law[*]

Aris L. Gulapa[**]

* This is an abridged and updated version of the author's thesis which was based on the problem in the 2002 Phillip C. Jessup International Moot Court *Compromis de Arbitrage*. The thesis was the recipient of the 2003 Dean's Award (*Silver Medal*) for Best Thesis.

** B.S. '99, J.D. '03, *With Honors*; *Ateneo Law Journal* Editorial Staff (2000-2003), Lead Editor (Vol. 47, Issue No. 3). The author deeply expresses his acknowledgment to the brilliant ideas of his adviser, Atty. Anton Elicaño. He wishes to thank Attys. Jose Victor Chan-Gonzaga (consultant); Katrina Diane Monsod (assistant adviser) and Sarah Lou Arriola for their contribution. He likewise extends his heartfelt gratitude to his contemporaries in the Ateneo Jessup Team (2001 & 2002) and the Ateneo Society of International Law, specifically Marie Camille Francesca Bautista; Mark Leinad Enojo; Archelle Lagsub; Geminiano Sandoval, Jr.; and Kirsten Jeanette Yap.

His past work published by the *Ateneo Law Journal* is entitled *The Jotting of Obiter Dicta in* Estrada v. Sandiganbayan: *Did the Supreme Court Blunder in its Decision on the Constitutionality of the Law on Plunder?*, 47 ATENEO L.J. 49 (2002).

Cite as 48 ATENEO L.J. 1051 (2004).

I. INTRODUCTION

The elimination of uncertainty in the application of accepted principles of international law shall endure, so long as the possible conjunction of facts remains infinitely various.[1] This remains true especially in this age where

1. BRIERLY, THE LAW OF NATIONS 68-76 (6d. 1963), *cited in* D.J. HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW 4 (5d. 1998) (discussing the concept of international law in the context of a changing environment); Richard Garnett, *Are Foreign Internet Infringers Beyond the Reach of the Law*, 23(1) U.N.S.W. L.J. 105, 105-6 (2000) (clarifying the impact of the Internet on domestic legislation); Henry Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILLANOVA L. REV. 1, 2 (1996) (recognizing that the Global Information Structure or G.I.I. made it more difficult to localize wrongdoing for purposes of criminal and civil litigation).

Conduct with potentially serious legal consequences is difficult for traditional sovereigns to control in the G.I.I. because it is ephemeral, invisible and crosses geographic boundaries easily. Geographically. based concepts of sovereignty must be squared with the nature of open networks, which are indifferent to geographic boundaries. Conventional doctrines of jurisdiction to prescribe, adjudicate, and to enforce legal decisions must evolve to handle new disputes in cyberspace.

rivers of information have deeply challenged accepted rules recognized by civilized nations.[2]

A. The Information Age

The dawn of the Information Age[3] has fundamentally transformed the way the world operates.[4] Most notably, the profound growth in use of the

2. *See id.* (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS §§ 402-33 [1987]) (explaining three types of jurisdiction) [hereinafter RESTATEMENT (THIRD)]. *See also* Ruth Wedgwood, *Cyber-Nations*, 88 KY. L.J. 957, 957-8 (1999/2000) ("It may be feckless to discuss statehood in anything other than an exhaustive account of how national movements have come to subsume territorial space."). *See generally* Joseph Burns, *Personal Jurisdiction and the Web*, 53 MELB. U. L. REV. 30, 31 (2001) (citing Christopher Gooch, *The Internet, Personal Jurisdiction, and the Federal Arm-Long Statute: Rethinking the Concept of Jurisdiction*, 15 ARIZ. J. INT'L & COMP. L. 635 [1998]) (emphasizing that there is an inherent difficulty in conceptualizing the Web). *Accord* Gwenn Kalow, *From the Internet to Court: Exercising Jurisdiction Over Wordl Wide Web Communications*, 65 FORDHAM L. REV. 2241 (1997); Leif Sedlow, Note, *Three Paradigms of Presence: A Solution for Personal Jurisdiction on the Internet*, 22 OKLA. CITY U. L. REV. 337 (1997).

See John Arquilla & David Ronfeldt, *Looking Ahead: Preparing for Information-age Conflict*, *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 493, 465-77 (1997), *cited in* George Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1195 ("The methodology of warfare may change during the Information Age that appears to be upon us. Responses to Internet-based attack may involve more than applying new strategies and tactics to threats and attacks and a beginning of major reductions in defense systems and infrastructure.") [hereinafter Walker, *Information Warfare*]. *See id.* (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS §§ 402-33 [1987]) (explaining three types of jurisdiction) [hereinafter RESTATEMENT (THIRD)]. *See also* Ruth Wedgwood, *Cyber-Nations*, 88 KY. L.J. 957, 957-8 (1999/2000) ("It may be feckless to discuss statehood in anything other than an exhaustive account of how national movements have come to subsume territorial space."). *See generally* Joseph Burns, *Personal Jurisdiction and the Web*, 53 MELB. U. L. REV. 30, 31 (2001) (citing Christopher Gooch, *The Internet, Personal Jurisdiction, and the Federal Arm-Long Statute: Rethinking the Concept of Jurisdiction*, 15 ARIZ. J. INT'L & COMP. L. 635 [1998]) (emphasizing that there is an inherent difficulty in conceptualizing the Web). *Accord* Gwenn Kalow, *From the Internet to Court: Exercising Jurisdiction Over Wordl Wide Web Communications*, 65 FORDHAM L. REV. 2241 (1997); Leif Sedlow, Note, *Three Paradigms of Presence: A Solution for Personal Jurisdiction on the Internet*, 22 OKLA. CITY U. L. REV. 337 (1997).

3. For an introduction to the Information Age, *see* ALVIN TOFFLER AND HEIDI TOFFLER, THE THIRD WAVE (1991) [hereinafter THE THIRD WAVE].

Internet has revolutionized the way individuals, societies, and governments communicate and conduct business.[5] Global communications cut across territorial borders; thus creating a new realm of human activity.[6] At the same time, the technology-intensive Information Age brings with it opportunities for destructive cyberactivities.[7] Attributes such as openness and ease of connectivity[8] that promote telecommunications efficiency and expedite customer service also now render society's information infrastructure vulnerable to new threats[9] from other computerized systems.[10]

To illustrate, shortly after the September 11 attack on the World Trade Center, the United States Government issued a warning that cyberattacks undermining America's critical information system could be launched by terrorists.[11] As prophesied, a group of Muslim hackers attacked a site

4. *Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Senate Commission on Government Affairs*, 104th Cong. 150, at 155 (1996). *See* ALVIN TOFFLER AND HEIDI TOFFLER, WAR AND ANTI-WAR 2 (1993).

5. Leslie Kurtz, *Copyright and The Internet – Word Without Borders*, 43 WAYNE L. REV. 117, 117 (1996) ("Around the world, efforts are being made to create rules of the road for what has been called the information superhighway.... [M]ade up of such elements as networks, computers, computer software, consumer electronics, and communication technology.... It is not a web created by any one person, group or entity, but rather a mass of separate technologies and developments that have grown together over the years and that are advancing at a remarkable pace."). *See* Christopher Joyner & Catherine Lotionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 825-867 (2001), *available at* http://www.ejil.org (last visited May 26, 2002) [hereinafter *Information Warfare as Interngtional Coercion*].

6. David Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996).

7. For an extensive discussion of, or treatise on, threats to national security, *see* JAMES ADAMS, THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE (1998) [hereinafter THE NEXT WORLD WAR].

8. Bruce Braun, et al., *WWW.Commercial_Terrorism.com: A Proposed Federal Criminal Statute Addressing the Solicitaion of Commercial Terrorism Through the Internet*, 37 HARV. J. LEG. 159, 159 (2000).

9. *See generally* Cilluffo et al., *Cybercrime ... Cyberterrorism ... Cyberwarfare: Averting an Electronic Waterloo, in* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES TASK FORCE REPORT (1998).

10. *See* US General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, REP. NO. GAO/T-AIMD-96-92 (1996) [hereinafter *Information Security*].

11. Ira Sager and John Carey, *Preparing for a Cyber-Assault*, BUSINESS WEEK, Oct. 22, 2001, at 50.

condemning the September 11 bombing and said they stood by bin Laden proclaiming, *"Osama bin Laden is a holy fighter, and whatever he says makes sense."*[12] A modified Web page warned that the group planned to hit major U.S. military and British Web sites and proclaimed an "Al-Qaeda Alliance Online." Another defacement contained similar messages along with images of badly mutilated children who had been killed by Israeli soldiers.[13]

As a matter of fact, more devastating cyberattacks occurred even prior to the post-September 11 cyberactivities. In 1998, the Emergency 911 systems of the U.S. did not escape the ire of cyberattackers when a young man from Sweden disabled portions of the Emergency 911 system in Southern Florida.[14] Further, the danger brought about by these digital criminals was typified when the Federal Airline Aviation control tower of the Worcester Regional Airport was disabled for six hours.[15]

Even a Filipino has drawn the attention of the entire international community because of the destructive 'I Love You' virus. In the year 2000, a student from a Philippine computer college released a hybrid virus and worm rapidly replicating itself through e-mail, overloading corporate e-mail systems in many countries and causing damage estimated at up to $10 billion.[16] Like the *Melissa*[17] and *Chernobyl*[18] worms, the 'I Love You' virus propagated itself through networks – in this case, e-mail. But unlike those two, it also destroyed and replicated itself by manipulating files on a user's

12. Dorothy Denning, *Is Cyber Terror Next, in* U.S. SOCIAL SCIENCE RESEARCH COUNCIL REPORT (2001), *available at* http://www.newsbytes.com (last visited May 30, 2002) [hereinafter Denning, *Is Cyber Terror Next*] ("The cyber attacks arising from the events of September 11 reflect a growing use of the Internet as a digital battleground. It is not at all unusual for a regional conflict to have a cyber dimension, where the battles are fought by self-appointed hackers operating under their own rules of engagement.").

13. *Id.*

14. *Hearings before the United States Senate Subcommittee on Technology, Terrorism, and Government Information Committee on the Judiciary*, 107th Cong. (2000) (statement of Frank J. Cilluffo, Deputy Director, Organized Crime Project Director, Task Force on Information Warfare & Information Assurance, Center for Strategic & International Studies).

15. *Id.*

16. *Love Bug Suspect Charged, at* http://www.usatoday.com/life/cyber/tech/cti167.htm (last visited May 2, 2002).

17. *Lawyer Likens the Melissa Virus to Graffiti*, N.Y. TIMES, Apr. 9, 1999, at B2.

18 *Taiwan College Says Ex-Student Wrote Chernobyl Virus Program*, N.Y. TIMES, Apr. 30, 1999, at A10.

hard drive, like a traditional virus.[19] The virus was first reported in Hong Kong and spread gradually west as a new day dawned, infecting government and business computers. In the U.S., the damage caused was estimated at $100 million in software damage. In Europe, the virus reached European parliaments, big companies, and financial traders, with more than 100,000 mailservers in Europe having been taken down by the virus.

The failure of the Philippine courts to prosecute the Filipino perpetrator had a catalytic effect on the enactment of the Philippine E-Commerce Act,[20] which penalized hacking and other computer-related crimes. However, recent global developments have shown the inadequacy of said law to deal with more violent cybercrimes, particularly, cyberterrorism. Thus, House Bill No. 3802 [21] was proposed in 2001 defining and criminalizing cyberterrorism. With the introduction of a House Bill on the definition of cyberterrorism, it becomes more imperative to lay down the elements comprising this crime to ensure that the Philippines would follow international norms defining this offense of a universal character.

B. The Threat

As cyber-systems assume increasingly complex,[22] more embedded roles in international commerce,[23] daily life,[24] and national defense, these computer networks have become more vulnerable to undetected attacks.[25] Today, the international community is concerned[26] about hostile foreign governments[27]

19. *ILOVEYOU Computer Bug Bites Hard, Spreads Fast, available on line at* http://www.cnn.com/2000/TECH/computing/05/04/iloveyou.01/1 (last visited May 28, 2002).
20. Republic Act No. 8792, 'An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions, Penalties for Unlawful Use Thereof and Other Purposes (2000).
21. H.B. 3802, 12th Cong. (1st Regular Sess. 2001).
22. Barry Kellman, *Terrorism and Business: An Introduction to Terrorism and Business*, 12 DEPAUL BUS. L.J. 21, 22 (2000)
23. Susan Lyman, Note, *Civil Remedies for the Victims of Computer Viruses*, 11 COMP. L.J. 607, 607 (1992) [hereinafter Lyman, *Civil Remedies*].
24. CHRIS REED, COMPUTER LAW 243 (3d. 1996) [hereinafter COMPUTER LAW].
25. *See Information Warfare: Defense*, U.S. DEFENSE SCIENCE BOARD TASK FORCE REPORT 2-15 (1996).
26. *See* Woolsey, *Resilience and Vulnerability in the Information Age, in* THE INFORMATION REVOLUTION AND NATIONAL SECURITY 79, 82-83 (Schwartzstein ed., 1996); Mann, *Cyber-Threat Expands with Unchecked Speed*, AVIATION WK. & SPACE TECH., Jul. 8, 1996, 63, at 64.

launching computer-based attacks on critical systems, *e.g.*, energy distribution, telecommunications and transportation systems, [28] which severely damage or disrupt national defense or other vital social services and result in serious harm to the public welfare.[29]

Malfunctioning of a vital information network infrastructure, for instance, military computer systems,[30] could readily paralyze a State.[31] Further, conduct adversely affecting the operation of a computer may likewise endanger passengers,[32] *e.g.*, penetrating an air traffic control system and causing two planes to collide.[33] Most disturbing is the fact that cyberattackers have targeted the financial world, a sector heavily dependent on computers,[34] causing the transfer of assets or the proceeds of crime from one jurisdiction to another,[35] or the interception of money in the process of

27. *See* Testimony of Director of Central Intelligence George J. Tenet, *Cyber Attack: Is the Nation at Risk?, Hearings before the Senate Committee on Government Affairs*, 105th Cong. at 10 (Jun. 24, 1998).
28. *See* Laqueur, *Postmodern Terrorism*, FOREIGN AFFAIRS, Sept.-Oct. 1996, at 14 [hereinafter Laqueur]. *See also* WINN SCHWARTAU, INFORMATION WARFARE: CHAOS ON THE ELECTRONIC HIGHWAY 308-310 (1994) [hereinafter SCHWARTAU].
29. Graham, *US Studies New Threat: Cyber Attack*, WASH. POST, May 24, 1998, A1 [hereinafter Graham]. *See* A student paper written by Jimmy Sproles and Will Byars for Computer Ethics at ETSU 1998, *at* http://www-cs.etsu-tn.edu/gotterbarn/stdntppr.html (last visited Apr. 15, 2002) (discussing the serious nature of Cyber Warfare and the security implications associated with the advancement of computers and computer technology as an implement of war) [hereinafter Sproles & Byars].
30. *See* Maier, *Is US Ready for Cyberwarfare?*, INSIGHT ON THE NEWS, Apr. 5, 1999, at 18.
31. Schwartau, *supra* note 24, at 308-310.
32. COMPUTER LAW, *supra* note 29, at 243.
33. Mark M. Pollitt, *Cyberterrorism: Fact or Fancy?*, *in* PROCEEDINGS OF THE 20TH NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE 285-289 (1997) [hereinafter Pollitt, *Fact or Fancy?*].
34. Marc Friedmann & Kenneth Buys, *Infojacking: Crimes on the Information Superhighway*, 13 COMP. L. 1, 7 n. 10 (1996).
35. *See* MARTIN WASIK, CRIME AND THE COMPUTER 187 (1991).

being transferred from one country to another.[36] Clearly, the international community faces new vulnerabilities as a result of this era.[37]

What have made States vulnerable to these new forms of attacks?

These new forms of attacks are a product of the rapid computerization of businesses and the military, and the revolutionary shift to large-scale networking of computers.[38] The heavy dependence[39] on computers by both governmental and private corporate networks[40] is a breeding ground for States and individuals, to experiment and expand their ability to cause terror. In the U.S., for example, the Pentagon reported 250,000 attacks on its computers in 1995, with 65% of those attempts yielding computer network entry.[41] In one event in 1994, hackers were able to gain access to Rome Laboratory's system, the Air Force's main command and control research center, with the resulting damage amounting to at least US$500,000.00. Through the Rome Laboratory system, the hackers gained access to NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base, and other government facilities, and stole critical Department of Defense (DOD) information, including air-tasking orders.[42]

Owing to the experiences, many States are preparing for cyberattacks, as this topic occupies a central role in national and international political and military planning.[43] However, for these States to resort to lawful responses

36. B.A.K. Rider, *Combating International Commercial Crime*, LLOYDS INT'L & MAR. L. Q. 217 (1985); ROSKILL REPORT, REPORT OF THE FRAUD TRIALS COMMITTEE (1986).

37. M. Cherif Bassiouni, *The Future of International Criminal Justice*, 11 PACE J. INT'L L. REV. 309 (1999). For a comprehensive disquisition on these threats, *see* MARK FINDLAY, THE GLOBALIZATION OF CRIME: UNDERSTANDING TRANSITIONAL RELATIONSHIPS IN CONTEXT (1999).

38. Neil Munro, *Sketching a National Information Warfare Defense Plan*, 39 Comms. of the ACM 15 (1996), LEXIS, Nexis News Library, Magpap File ("The nation's myriad of computer-controlled networks, the phone switches, the power grid, the air-traffic control system, the banks, can all be wrecked during a war or crisis by hostile hackers funded and protected by countries such as Iran ....").

39. Arnaud de Borchgarve, *Hackers Probed in Failure of Satellite, International Group Has Made Threats*, WASH. TIMES, May 23, 1998, at A1.

40. Seth Schiesel, *Millions Await Beep But Box Remains Silent*, N.Y. TIMES, May 21, 1998, at A1.

41. *Information Security*, *supra* note 10.

42. Pierre Thomas & Elizabeth Corcoran, *Argentine, 22, Charged with Hacking Computer Networks*, WASH. POST, Mar. 30, 1996, at A4.

43. D. Waller, *China's Arms Race*, TIME, Jan. 25, 1999, *at* cgi.pathfinder.com/time/asia/magazine/1999/990125/Chinese_military2.html (last visited Apr. 16, 2002); G. Browning, *Infowar*, THE DAILY FED, Apr. 21, 1997, *at* www.govexec.com/dailyfed/0497/042297b1.htm (last visited Apr. 16, 2002); D. Verton, *Should the U.S. Continue to Plan Enemy Attacks via Cyberspace?*, CNN Interactive federal Computer Week, Jan. 6, 1999, *at* www.cnn.com/TECH/computing/9901/06/infowar.idg/index.html (last visited Apr. 16, 2002) ; M. Bunker, *Will Hackers or Spies Knot the Net*, MSNBC, Jul. 23, 1998, *at* www.msnbc.com/news/177668.asp (last visited Apr. 16, 2002).

against cyberattacks and their perpetrators, it is necessary to identify varying degrees of cyberattacks, and evaluate them under international law.

In crafting a legal framework concerning responses to varying degrees of cyberattacks, it is crucial to answer the following questions: What are the varying degrees of cyberattacks? What constitutes cyberterrorism? Does the use of cyberforce constitute a violation of the proscription against the 'use of force' under the U.N. Charter? May a cyberattack qualify as an "armed attack" to trigger the right of self-defense under international law?

The importance of identifying and evaluating cyberattacks is to provide a clear framework to any cyberattacked State as to how to lawfully respond to these new forms of attack. This paper attempts to enlighten States, including the Philippines, as to their obligations and responsibility with respect to certain types or forms of cyberattacks. While some cyberattacks would remain within domestic concerns, an attack constituting cyberterrorism would present pressing issues on the duty of States to prevent and suppress acts of terrorism.

In addition, attacks constituting "cyber-use of force" have serious international implications. The determination of what constitutes "Use of Force" in the Information Age is significant in two respects. First, it assists in determining when the attacked State may be entitled to exercise self-defense or some lesser form of sanction against one who engages in cyberattacks.[44] Corollarily, it puts any State on notice as to when its own conduct may legitimately be described as a use of force amounting to an armed attack, thereby entitling other nations to take self-defense or other appropriate measures.[45] At present, it seems that international rules do not give the State the precise answers in dealing with many of these issues.[46]

44. Richard W. Aldrich, *How Do You Know You Are at War in the Information Age?*, 22 HOUS. J. INT'L L 223 (2000) (explaining that the use of cyber-means may not produce immediate death and destruction of property, but may innocuously manipulate bits of data, changing ones to zeros and vice versa, to deleterious effect nonetheless) [hereinafter Aldrich, *War in the Information Age*].

45. LOUIS HENKIN, HOW NATIONS BEHAVE: LAW AND FOREIGN POLICY 285-96 (2d. 1979).

46. Richard W. Aldrich, *The International Legal Implications of Information Warfare*, AIRPOWER J. 99, 99-101 (1996) [hereinafter Aldrich, *The International Legal Implications*].

In the same vein, the rise of cyberattacks constituting cyberterrorism and cyber-use of force provokes questions about the parameters of an "armed attack" and "self-defense," as articulated in the U.N. Charter.[47] The highly destructive potential of cyberattacks underscores the altered nature of the globally interconnected environment, as well as the technological revolution in how transnational conflict might be conducted in the Information Age. These developments only highlight the need to develop or amend the rules and criteria upon which factual assertions are based for a State to employ force against another State. The nature of cyberattacks suggests that, while international legal norms found in contemporary U.N. Charter law are helpful, they may not be adequate in reaching acceptable solutions.[48]

It must likewise be noted that attribution and State participation exist along a wide spectrum.[49] A cyberattack might be initiated by a foreign private entity or person without State-sponsorship, or a foreign State could simply hire mercenary-like individuals or acknowledge and adopt the conduct of an individual in carrying out a cyberattack.

47. *See* Allard, *The Future of Command and Control: Towards a Paradigm of Information Warfare*, *in* TURNING POINT: THE GULF WAR AND US MILITARY STRATEGY 161, 166 (Benjamin Ederington & Michael J. Mazarr eds., 1994); DEPARTMENT OF DEFENSE, CONDUCT OF THE PERSIAN GULF CONFLICT: FINAL REPORT TO CONGRESS (1992); Swalm, *Joint STARS in Desert Storm*, *in* THE FIRST INFORMATION WAR 167 (Alan D. Campen ed., 1992).

48. *Information Warfare as International Coercion*, *supra* note 5 (citing Vizard, *War.Com: A Hacker Attack Against NATO Uncovers a Secret War in Cyberspace*, POPULAR SCIENCE, Jul. 1, 1999, at 80) [hereinafter Vizard]. The Charter was designed for military conflicts involving large-scale armed attacks by one State against the territory of another, such as those in the First World War, the Second World War and on smaller scales throughout the Cold War. During those times, States could count an enemy's planes, tanks and ships. From these assessments, a government could decide how to organize its defense based upon its determination of imminence of the enemy's offensive threat capabilities. The use of cyber-means makes the determination of an enemy's assets more difficult and thus complicates arrangements for setting up adequate defensive strategies. It is difficult to manage risks in conflict or to know what assets must be spent on defense, especially when who, where or what IW weapons an enemy possesses remain unknown factors. *See also* Rattray, *The Emerging Global Information Infrastructure and National Security*, *in* FLETCHER FORUM ON WORLD AFFAIRS 81, 93-95 (1997) (describing the need for multilateral efforts to control information warfare and positing several different international mechanisms). *But see* Anthony Lake, 6 NIGHTMARES 57 (2000).

49. *See* James Crawford, *Revising the Draft Articles on State Responsibility*, 10 EUR. J. INT'L L. 435, 435 n. 2 (1999) [hereinafter Crawford]. *See also* International Law Commission, U.N. Press Release, 18th Meeting, GA/L/3158 (2000).

Finally, in their efforts to combat terrorists, States may themselves commit human rights violations.[50] States, incapable of dealing with crime in general, may not respond effectively and appropriately to terrorism.[51] This would include resort to kidnapping or forcible abduction, or other forms or irregular rendition, of terrorists. While terrorists are a clear threat to the very concept of human rights underlying the creation of the United Nations,[52] international human rights law appears to restrain States in their vigorous attempts to capture these human rights violators.

Under these circumstances, what lawful responses may a State resort to?

II. TERRORISM AND THE RISE OF A NEW MODE OF INFLICTING HARM AND VIOLENCE

The arsenal available to today's terrorist is expanding, allowing greater sophistication in the ability to carry out devastating acts.[53] Terrorist and outlaw States have extended the world's fields of battle, from physical space to cyberspace, from earth's vast bodies of water to the complex workings of the human body.[54]

50. David Weissbrodt, *Human Rights and Responsibilities of Individuals and Non-State Entities*, *in* JUSTICE PENDING: INDIGENOUS PEOPLES AND OTHER GOOD CAUSES, ESSAYS IN HONOUR OF ERICA-IRENE DAES 239, 257 (2002).

51. DEMOCRACY AND TERRORISM 205-207 (G.N. Srivastava ed., 1997).

52. Kalliopi Koufa, *Human Rights and Terrorism in the United Nations*, *in* JUSTICE PENDING: INDIGENOUS PEOPLES AND OTHER GOOD CAUSES, ESSAYS IN HONOR OF ERICA-IRENE DAES 203, 213 (2002).

53. *See* Barry Kellman, *Bridging the International Trade of Catastrophic Weapons*, 43 AM. U. L. REV. 755 (1994).

54. Bill Clinton, Remarks before the National Academy of Sciences in Washington D.C. (Jan. 22, 1999). In said speech, Clinton stated:

> The enemies of peace realize they cannot defeat us with traditional military means. So they are working on two new forms of assault, which you've heard about today: cyberattacks on our critical computer systems, and attacks with weapons of mass destruction – chemical, biological, potentially even nuclear weapons. We must be ready – ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services – or military assets. More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption. Last spring, we saw the enormous impact of a single failed electronic link, when a satellite malfunctioned – disabled pagers, ATMs, credit card systems and television networks all around the world. And we already are seeing the first wave of deliberate cyber attacks – hackers break into government and business computers, stealing and destroying information, raiding bank

Two types of terrorism have surfaced: conventional terrorism and catastrophic terrorism.[55] Conventional terrorism refers to the use of physical terror-violence, such as plane hijacking, kidnapping, or bombing with conventional explosives causing numerous casualties. [56] In contrast, catastrophic terrorism is the use of non-conventional means, *i.e.* nuclear, chemical, biological, radiological weapons, and until recently, *cyberterrorism*, capable of, and typically intended to be, causing casualties in the thousands or an extraordinary suspension of civilized order.[57] Catastrophic terrorism is an intentionally undefined term, reflecting the fact that terrorists who aspire to inflict catastrophic injuries have a wide menu of options to employ, and reflecting the conclusion that debates over whether a particular technology is or is not within this category are, essentially, inconclusive.[58] The definition of "catastrophic terrorism," as opposed to conventional terrorism, turns less on what type of device is used than on the magnitude of the effects.

A. The International Crime of Terrorism

Even before the dawn of the Information Age, States have been obliged under customary international law to cooperate with other States in order to maintain peace and security. [59] Terrorism is one international crime [60]

accounts, running up credit card charges, extorting money by threats to unleash computer viruses.

55. Barry Kellman, *Catastrophic Terrorism – Thinking Fearfully, Acting Legally*, 20 MICH. J. INT'L L. 537, 537 (1999) [hereinafter Kellman, *Thinking Fearfully, Acting Legally*].

56. *See generally* M. Cherif Bassiouni, *Terrorism and Business: Forward: Assessing "Terrorism" into the New Millennium*, 12 DEPAUL BUS. L.J. 1, 11 (2000).

57. *See* Barry Kellman & David Gualtieri, *Barricading the Nuclear Window – A Legal Regime to Curtail Nuclear Smuggling*, 1996 U. ILL. L. REV. 667, 667-9 (1996). *See also* Laqueur, *supra* note 28; Ashton Carter, et al., *Catastrophic Terrorism: Tackling the New Danger*, WASH. Q., Nov.-Dec. 1998, at 80.

58. Kellman, *Thinking Fearfully, Acting Legally*, *supra* note 55, at 537.

59. Measures to Prevent International Terrorism which Endangers or Takes Innocent Human Lives or Jeopardizes Fundamental Freedom, G.A. Resolution 38/130, 38 U.N. GAOR Supp. (No. 47) 266-7, U.N. Doc. A/38/47 (1984); I OPPENHEIM, INTERNATIONAL LAW 292-3 (Lauterpacht ed., 1955) [hereinafter OPPENHEIM].

60. *See* Jessica Howard, *Invoking State Responsibility for Aiding the Commission of International Crimes – Australia, the United States and East Timor*, 2 MELBOURNE J. INT'L L. 1, 11 (2001) [hereinafter *Invoking State Responsibility*]. *See generally* ILC Report of the International Law Commission on the Work of its 28th Session, II Y.B.I.L.C. 67 (1976).

breaching international peace and tranquility. [61] Using fear as its tool, terrorists have demonstrated their ability to sow violence and destruction[62] and bring large communities to a standstill.[63] The atrocious consequences of terrorism have been illustrated by the *Lockerbie Incident*,[64] in which Pan American Flight 103 was brought down by an explosive planted in a cassette player and loaded into the plane's baggage compartment, killing more than 250 people on board and on the ground.[65]

It is interesting to note that the international community's response to acts of terror-violence has traditionally been influenced by sensational events,[66] such as the 1993 bombing of the World Trade Center in New York,[67] the 1995 bombing of the Federal Building in Oklahoma City,[68] and the 1998 bombings of the American embassies in Kenya and Tanzania.[69] Consequently, the Security Council has called on States to ensure that all terrorists are brought to justice,[70] while the General Assembly has ordered States to take measures to eliminate international terrorism.[71] Even the U.N.

61. S.C. Res. 1368, U.N. Doc.S/RES/1368 (2001). *See Legal Regulation of Use of Force*, 96 AM. J. INT'L L. 237, 244 (2002) ("At the United Nations, the Security Council unanimously adopted on September 12 a resolution condemning the horrifying terrorist attacks, which the Council regarded, like any act of international terrorism, as a threat to international peace and security.").

62. Vienna Declaration and Programme of Action, Part I., para. 17, U.N. Doc. A/CONF.157/24 (1993).

63. Michael Reismann, Comment, *In Defense of World Public Order*, 95 AM. J. INT'L L. 833, 834 (2001).

64. Case Concerning Questions of Interpretation and Application of the Montreal Convention Arising out of the Aerial Incident at Lockerbie (Libya v. U.K.), 1992 I.C.J. 3 (Provisional Measures).

65. *See* Her Majesty's Advocate v. Al Megrahi, (H.C.J. 2001) Case No. 1475/99, at 1 (Scot.).

66. *See* M. Cherif Bassiouni, *Media Coverage of Terrorism*, 32 J. OF COMM. 128, 128-9 (1982).

67. *Constructing a Trail to the Bombers*, NEWSWEEK, Mar. 8, 1993, at 25.

68. Evan Thomas, et al., *The Manhunt: Cleverness – and Luck*, NEWSWEEK, May 1, 1995, at 30.

69. Hugh Dellios, *Bombs Rip U.S. Embassies; More than 80 Killed, 1,600 Hurt as Explosions Rock Kenyan, Tanzanian Capitals; Rescuers Struggle Amid Rubble, Carnage*, CHI. TRIB., Aug. 8, 1998, at N1.

70. S.C. Res. 748, U.N. SCOR, 47th Sess., U.N. Doc. S/23992 (1992).

71. U.N. Doc. A/Res/40/61 (1985).

High Commission on Human Rights has appealed to States to prevent such acts as they violate the rights of innocent civilians.[72]

1. The U.N. General Assembly's Condemnation of all Terrorist acts

Opinio juris may be deduced from the attitudes of States towards the adopted text of U.N. Resolutions.[73] As a matter of fact, the effect of consent to the text of such Resolutions is not merely that of reiteration or elucidation of Charter obligations, but as an acceptance of the validity of the rule or set of rules declared by the Resolutions themselves.[74]

Although the General Assembly's power seems recommendatory in promoting international cooperation,[75] the traditional opinion that all G.A. resolutions are not a source of international law[76] has long been discarded.[77] Certain G.A. Resolutions may become sources of international obligations

72. Mary Robinson, Protecting Human Rights: The U.S., the U.N., and the World, U.N. High Commissioner Lecture at the JFK Library, Boston (Jan. 6, 2002); Press Release, Terrorism Require Response Founded on Inclusion, Fairness, Legitimacy, General Assembly Told As Debate Continues, 56th General 15th Plenary Meeting (2001).

73. Ross Schreiber, *Ascertaining* Opinio Juris *of States Concerning Norms Involving the Prevention of International Terrorism: A Focus on the U.N. Process*, 16 B.U. INT'L L.J. 309, 325 (1998) [hereinafter *Ascertaining* Opinio Juris].

74. Military and Paramilitary Activities (Nicaragua v. U.S.), 1986 I.C.J. 100.

75. U.N. CHARTER, art. 13(1)(a).

The General Assembly shall initiate studies and make recommendations for the purpose of:

a. promoting international cooperation in the political field and encouraging the progressive development of international law and its codification;
b. promoting international cooperation in the economic, social, cultural, educational, and health fields, and assisting in the realization of human rights and fundamental freedoms for all without distinction as to race, sex, language or religion.

76. *See generally* Sloan, *General Assembly Resolutions Revisited*, 58 B.Y.I.L. 39, 39 (1987) (citations omitted) [hereinafter Sloan], *cited in* HARRIS, CASES AND MATERIALS, *supra* note 1, at 58.

77. HARRIS, CASES AND MATERIALS, *supra* note 1, at 62 (citing Letter by Mr. Schwebel, Deputy Legal Adviser of the U.S. Department of State, 1975 U.S.D.I.L. 85) (stating that to the extent, which is exceptional, that such resolutions are meant to be declaratory of international law, are adopted with the support of all members, and are observed by the practice of States, such resolutions are evidence of customary international law on a particular subject matter).

when they are adopted unanimously or by a large and representative majority.[78] States voting for a particular Resolution are bound on the grounds of consent,[79] while those abstaining are bound by acquiescence and tacit consent, since an abstention is not a negative vote.[80] This cannot be denied as even the World Court admits the legally binding force of certain G.A. resolutions, such as in the *Namibia Advisory Opinion*[81] or the *Western Sahara Advisory Opinion*.[82] The terms of the Resolution itself are a factor in giving the resolution its weight under international law.[83]

Action by the General Assembly against terrorism can be traced to the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance With the U.N. Charter, in which it was agreed that every State had the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or

78. YUWEN LI, TRANSFER OF TECHNOLOGY FOR DEEP SEA-BED MINING: THE 1982 LAW OF THE SEA CONVENTION AND BEYOND 33 (1994) (explaining how the 1970 Declaration of Principles Governing the Sea Bed and the Ocean Floor Beyond the Limits of National Jurisdiction evince hard law).

Such resolutions formulate new principles which may eventually lead to international treaties or new customs. Bin Cheng identified this particular type of U.N. resolution as instant international customary law. In his view, such resolutions can serve as midwives for the delivery of nascent rules of international customary law which form within the United Nations. *Id.*

79. Sloan, *General Assembly Resolutions, supra* note 76; SOHN, THE PRESENT STATE OF INTERNATIONAL LAW AND OTHER ESSAYS 39 (Bos ed., 1973) ("In a rapidly changing world, the United Nations has found a method, albeit restricted by the rule of unanimity or quasi-unanimity, to adapt the principles of its Charter and the rules of customary international law to the changing times with an efficiency which even its most optimistic founders did not anticipate.").

80. YUWEN LI, TRANSFER OF TECHNOLOGY, *supra* note 78, at 31.

81. Advisory Opinion on the Legal Consequences for States of the Continued Presence of South Africa in Namibia,1971 I.C.J. 16.

82. Western Sahara Advisory Opinion, 1975 I.C.J. 31-32.

83. Declaration of the United Kingdom, U.N. GAOR, 29th Sess., U.N. Doc.A/C.6/SR.1492 (1974) ("Many resolutions were of such a nature and had such a content that they could have no, relevance to the development of international law.") [hereinafter Declaration of the United Kingdom]. *See* Declaration of the Mexico, U.N. GAOR, 29th Sess., U.N. Doc.A/C.6/SR.1486 (1974) ("Those and many other General Assembly declarations and resolutions of a similar type reflected the desire of Members States to promulgate juridical rules of unquestionable validity to which they all subscribed....") [hereinafter Declaration of the Mexico]. *Accord* Declaration of Iraq, U.N. GAOR, 29th Sess., U.N. Doc.A/C.6/SR.1486 (1974) [hereinafter Declaration of Iraq].

terrorist acts in another State.[84] This was followed by G.A. Resolution 3034, which invited States to take measures on both the national and international levels against terrorism.[85]Various Resolutions were subsequently adopted condemning the same acts.[86]

Ultimately, G.A. Resolution 34/145 was adopted condemning the continuation of repressive and terrorist acts and called upon all States to refrain from organizing, instigating, assisting, or participating in acts of civil strife or terrorist acts in another State, or acquiescing in organized activities within their territory directed towards the commission of such acts.[87] It was adopted by a record vote of 118 to 0, with 22 abstentions.[88]

Prior to G.A. Resolution 34/145, no consensus as to the condemnation of terrorist acts had been reached owing to differences in opinion as to the definition of terrorism, and the confusion of the term with national liberation movements. By Resolution 34/145, the Assembly adopted the recommendations of the *Ad Hoc* Committee specially created for the prevention of terrorist acts, hence, condemning all acts of repressive and terrorist acts and finally incorporated the express language of the Declaration on Friendly Relations regarding terrorism.[89]

Interestingly, Resolution 40/61, adopted in 1985, introduced more embracing language. For the first time, it unequivocally condemned, as criminal, *all acts, methods and practices* of terrorism, *wherever and whenever* committed, including those which jeopardize friendly relations among States and their security.[90] This was reaffirmed by Resolution 42/159, adopted by a

84. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance With the U.N. Charter, Annex to G.A. Resolution 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N. Doc.A/8028 (1970) [hereinafter Friendly Relations].

85. G.A. Res. 3034, U.N. GAOR, 27th Sess., Supp. No. 30, at 1, U.N. Doc. A/RES/3034 (1973).

86. G.A. Res. 31/102, U.N. GAOR, 31st Sess., Agenda Item 113, at 1, U.N. Doc.A/RES/102 (1976); G.A. Resolution 32/147; U.N. GAOR, 32nd Sess., Agenda 118, at 1, U.N. Doc.A/RES/147 (1978).

87. G.A. Res. 34/145, U.N. GAOR, 34th Sess., Agenda Item 112, ¶ 3, at 2, U.N. Doc.A/RES/145 (1980).

88. In any case, the abstentions were rendered moot as two years later Resolution 36/109 containing the same language was adopted without a vote. *See* G.A. Res. 36/109, U.N. GAOR, 36th Sess., Agenda Item 114, at 2, U.N. Doc.A/RES/36/109 (1981).

89. G.A. Res. 34/145, U.N. GAOR, 34th Sess., Agenda Item 112, ¶ 3, at 2, U.N. Doc. A/RES/34/145 (1980). *See Ascertaining* Opinio Juris, *supra* note 73, at 322.

90. G.A. Res. 40/61, U.N. GAOR, 40th Sess., Agenda Item 129, at 3, U.N. Doc.A/RES/40/61 (1981).

vote of 153 to 2, and 46/51 in 1987.[91] The condemnation of terrorism as criminal in the text of at least three Resolutions (40/61, 42/159, and 46/51) indicates a recognition of the duty of States to prosecute terrorists regardless of the nationality of the terrorist, the place where the act of terrorism is committed, and *the manner by which it is inflicted*.[92]

1. The Security Council and the Obligation to Bring Terrorists to Justice

The maintenance of international peace and security is, as Article 1(1) of the Charter indicates, the most important goal of the U.N.[93] Chapter VII empowers the Security Council to take some action with respect to threats to, and breach of, the peace.[94] Not surprisingly, the Security Council has played an active role in pursuing terrorists.[95] For instance, the Council has required Libya to return the alleged terrorist offenders and imposed sanctions against it for not doing so,[96] as the Council found Libya as having engaged in international terrorism.[97]

Any doubts as to the illegality of terrorist acts have been put to rest by the recent terrorist attack on the World Trade Center.[98] It has provoked the Security Council, through Resolution 1368, to unequivocally condemn the terrorist attacks and regard such acts, like any act of international terrorism, as a threat to international peace and security.[99] The Council further called on all States to work together urgently to bring to justice the perpetrators, organizers, and sponsors of these terrorist attacks and *stressed* that those responsible for aiding, supporting, or harbouring the perpetrators, organizers, and sponsors of these acts would be held accountable.

Subsequently, the Security Council adopted Resolution 1373, declaring that States shall prevent, suppress, and criminalize the financing of terrorist acts, and prohibit their nationals or any persons or entities within their

91. G.A. Res. 42/159, U.N. GAOR, 42nd Sess., Agenda Item 126, at 1, U.N. Doc.A/RES/42/159 (1987).

92. *Ascertaining* Opinio Juris, *supra* note 73, at 326.

93. U.N. CHARTER, art. 1(1).

94. BRUNO SIMMA, THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 608 (1994) [hereinafter SIMMA]

95. *See* Letter dated October 7, 2001 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, U.N. Doc.S/2001/946 (Oct. 7, 2001).

96. S.C. Res. 748, U.N. SCOR, 47th Sess., U.N. Doc.S/23992 (1992).

97. HARRIS, CASES AND MATERIALS, *supra* note 1, at 1041.

98. *See generally Responding to Terrorism: Crime, Punishment and War*, 115 HARV. L. REV. 1217, 1218 (2002).

99. S.C. Res. 1368, U.N. Doc.S/RES/1368 (2001).

territories from making financial assets or economic resources available to terrorists.[100] It also decided that all States shall refrain from supporting terrorists, deny safe haven to those involved in such acts, and ensure that any person who participates in such acts is brought to justice.[101]

3. International and Regional Conventions: Terrorists as Outlaws

Treaty law has repeatedly outlawed terrorism.[102] As early as 1937, after the assassination of French statesman Jean-Louis Barthou and King Alexander of Yugoslavia in Marseilles in 1934,[103] the League of Nations adopted the first convention on terrorism.[104] Twenty-four States were signatories to this convention, though it is telling that only one state, India,[105] ratified it.

The growth of civil aviation after World War II made civilian aircraft vulnerable targets for hijacking and sabotage.[106] The international community reacted to the large number of aircraft hijacking and sabotage incidents with fear and determination, resulting in a number of international

100. S.C. Res. 1373, U.N. Doc.S/RES/1373 (2001).

101. *Id.*

102. Abramovsky, *Multilateral Conventions for the Suppression of Unlawful Seizure and Interference with Aircraft: The Hague Convention*, 13 COLUM. J. TRANSNAT'L L. 398-399 (1974). *See also* New York Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons including Diplomatic Agents, 28 U.S.T. 1975, T.I.A.S. No. 7570 (1973); Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 24 U.S.T. 564 (1971); Convention to Prevent and Punish Acts of Terrorism Taking the Forms of Crimes Against Persons and Related Extortion that are of International Significance, O.A.S. Doc. A/6/Doc. 88 rev. 1, corr.1 (Feb. 2, 1971), *reprinted in* 10 I.L.M. 255 [hereinafter Convention on Terrorism Taking the Forms of Crimes Against Persons]; International Convention Against the Taking of Hostages, G.A Res. 146, U.N. GAOR, 34th Sess., Supp. No. 39 (1979); European Convention on the Suppression of Terrorism, Europ T.S. No. 90, *reprinted in* 15 I.L.M. 1272 (1977) [hereinafter European Convention on the Suppression of Terrorism].

103. Joel Cavicchia, *The Prospects for an International Criminal Court in the 1990s*, 10 DICK. J. INT'L L. 223, 225 (1992); Cherif Bassiouni, *The Time Has Come for an International Criminal Court*, 1 IND. INT'L & COMP. L. REV. 1, 4 (1991).

104. League of Nations, Convention for the Prevention and Punishment of Terrorism, Doc. C.546(I), O.J. 19 at 23 (1938).

105. *See also* M. Cherif Bassiouni, *International Terrorism*, *in* 1 INTERNATIONAL CRIMINAL LAW 765 (M. Cherif Bassiouni ed., 1999).

106. Alona Evans, *Aircraft Hijacking: Its Cause and Cure*, 63 AM. J. INT'L L. 695 (1969).

conventions adopted between 1969-1988.[107] That same period also witnessed a rapid increase in the kidnappings of civilian hostages for ransom, resulting in the adoption of a specialized United Nations Convention in 1979.[108] Similarly, a series of assassinations and kidnappings of diplomats from the 1960s to the 1990s brought about the adoption of several multilateral conventions.[109]

The seizure of the Italian vessel Achille Lauro on the high seas then led to the adoption of the Convention Against Unlawful Acts in Maritime Navigation in the mid-1980s. Recently, the American Embassy bombings in Kenya and Tanzania similarly prompted the 1998 adoption of the International Convention for the Suppression of Terrorism Bombings, which criminalizes terrorist attacks upon State or government facilities.[110]

Various regional conventions[111] likewise seek to prevent terrorist acts of violence in the same manner. These Conventions have directly attached liability to individuals who have threatened civilians with death or severe

107. Convention on Offences and Certain Other Acts Committed on Board Aircraft, 704 U.N.T.S. 219 (1963); Convention for the Suppression of Unlawful Seizure of Aircraft, 860 U.N.T.S. 105 (1970); Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 974 U.N.T.S. 177 (1971); Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving Civil Aviation, ICAO Doc. 9518, *reprinted in* 27 I.L.M. 627 (1988).

108. International Convention Against the Taking of Hostages, U.N. GA Res. 34/154 (XXXIV), U.N. GAOR, 34th Sess., Supp. No. 46 at 245, U.N. Doc. A/34/146 (1979), *reprinted in* 18 I.L.M. 1456.

109. Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, 1035 U.N.T.S. 167 (1973); Convention on the Safety of United Nations and Associated Personnel, G.A. Res. 59, U.N. GAOR, 49th Sess., U.N. Doc. A/49/59 (1994). *See also* Convention on Terrorism Taking the Form of Crimes Against Persons, *supra* note 102.

110. International Convention for the Suppression of Terrorism Bombings, G.A. Res. 165, U.N. GAOR, 52nd Sess., art. 2, U.N. Doc. A/52/164 (1998).

111. European Convention on the Suppression of Terrorism, *supra* note 102; Organization of African Unity, Draft Convention of the Organization of African Unity on the Prevention and Combating of Terrorism, CAB/LEG/24.14/Vol.I/Rev.3 (1999); Arab Convention for the Suppression of Terrorism, Adopted by the Council of Arab Ministers of the Interior and the Council of Arab Ministers of Justice at Cairo, Egypt (Apr. 1998) *available at* http://www.lasmediaservice.htm (last visited Jul. 14, 2002); Member States of the South Asian Association for Regional Cooperation, Regional Convention on Suppression of Terrorism, U.N. GAOR 6th Comm., 44th Sess., U.N. Doc. A/51/136(1989).

injury.[112] While recognizing the legitimacy of the struggle for national liberation,[113] the international community refused to condone these methods of pursuing political objectives as being contrary to the right to life, liberty, and security.[114] For these States, no goal or cause is so noble that it could justify all possible means,[115] specifically violence.[116]

B. The Definition of Terrorism

Academic discussions of terrorism begin by explaining that a universally accepted definition of the term still eludes scholars and government officials.[117] One survey of leading researchers uncovered 109 different definitions;[118] a mere compilation of these would readily comprise a tome.[119]

Despite debate over the definition, core characteristics of the term are agreed upon within the literature: the use of threat and/or violence, the existence of a political motive, the selection of targets who are representative of a target category, the aim of terrorizing, the goal of modifying behavior, the use of extreme or unusual methods, and the use of terrorism as an act of communication.[120] These elements have been recently codified by the General Assembly in its definition of terrorism in a Resolution adopted without a vote, to wit:

112. Wil Verwey, *The International Hostages Convention and National Liberation Movements*, 75 AM. J. INT'L L. 69, 70 (1981).

113. Declarations of Egypt, Tanzania, Guinea, Libyan Arab Jamahiraya. Nigeria, and Lesotho, U.N. Doc. A/32/39, at 39, 35 (1981).

114. Declaration of Chile, Mexico, Egypt, Guinea, and Iran, U.N. Doc.A/32/39, at 17, 21, 26, 38, 39 and 40 (1981).

115. Declaration of the United States, U.N. Doc. A/32/39, at 53 (1981).

116. *See* Jimenez v. Aristeguieta, 311 F.2d 547 (5th Cir., 1962), *cert. den.*, 375 U.S. 48 (1963).

117. A. Odasuo Alali & Kenoye Kelvin Eke, *Introduction: Critical Issues in Media Coverage of Terrorism, in* MEDIA COVERAGE OF TERRORISM: METHODS OF DIFFUSION 3 (Alali & Kenoye eds., 1991); Sharryn J. Aiken, *Manufacturing 'Terrorists': Refugees, National Security and Canadian Law – Part 1*, REFUGE: CANADA'S PERIODICAL ON REFUGEES, Dec. 3, 2000, at 65; Susan Dente, *In the Shadow of Terror: The Illusive First Amendment Rights of Aliens*, 6 COMM. L. & POL'Y 82 (2001).

118. Ray Takeyh, *Two Cheers from the Islamic World*, FOREIGN POL'Y, Jan.-Feb. 2002, at 70-1.

119. Shaukat Qadir, *The Concept of International Terrorism: An Interim Study of South Asia, in* ROUND TABLE 333-9 (2001).

120. Rachel Monaghan, *Single-Issue Terrorism: A Neglected Phenomenon*, STUDIES IN CONFLICT AND TERRORISM, Oct.-Dec. 2000, at 256.

> Criminal acts intended or calculated to provoke *a state of terror* in the general public, a group of persons or particular persons *for political purposes* are in any circumstances unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious, or other nature, that may be invoked to justify them.[121]

This definition was carefully arrived at after a thorough examination of numerous multilateral treaties and domestic legislation. It finds support in Article 24 of the International Law Commission's Draft Code of Crimes against the Peace and Security of Mankind,[122] which was derived from the 1937 Convention for the Prevention and Punishment of Terrorism,[123] which, in turn, defines acts of international terrorism as "acts against another state directed at persons or property and of such nature as to create a state of terror in the minds of public figures, groups of persons, or the general public."[124] Drafts of the Commission have been said to constitute evidence of a custom,[125] especially when affirmed by similar definitions found in international and regional conventions.[126] Concomitantly, the employment of excessive terror-generating violence in order to achieve a political purpose has been internationally censured, removing it from the domain of domestic concern.[127]

121. Measures to Eliminate Terrorism, G.A. Resolution 51/210, 88th Plenary Mtg., Item I.2, U.N. Doc. A/52/210 (1996) (emphasis supplied).

122. ILC Draft Code of Crimes Against the Peace and Security of Mankind, U.N. Doc. A/46/10/238, *reprinted in* 1 CHERIF BASSIOUNI, INTERNATIONAL CRIMINAL LAW Appendix 1 (1986).

123. LEAGUE OF NATIONS, art. 1 (2), 19 O.J. 23 (1938). However, this Convention did not take effect.

124. CHRISTOPHER BLAKESLEY, TERRORISM, DRUGS, INTERNATIONAL LAW AND THE PROTECTION OF HUMAN LIBERTY 310-311 (1992) [hereinafter BLAKESLEY, TERRORISM].

> It includes bombings, kidnappings, assassinations, hijackings, violations of diplomatic immunity, the holding of hostages, and so on. Terrorism may reflect a variety of motivations – national liberation, irredentism, and succession; ideological goals of the left and right...; Latin American drug cartels against rival parties, incumbent governments, police forces, MNC's capitalism and socialism; fundamentalist and/or revolutionary religious rage against implacable enemies...

125. MALCOLM SHAW, INTERNATIONAL LAW 93 (2d. 1986) [hereinafter SHAW].

126. *Extradition in an Era of Terrorism: The Need to Abolish the Political Offense Exception*, 61 N.Y.U. L. REV. 654, 654 (1986).

127. *See generally* GILBERT GEOFF, ASPECTS OF EXTRADITION LAW 129 (1990) [hereinafter ASPECTS]; GILBERT GEOFF, TRANSNATIONAL FUGITIVE OFFENSES IN INTERNATIONAL LAW: EXTRADITION AND OTHER MECHANISMS 205 (1998).

Although a municipal law has yet to be passed by Congress, the Philippines adheres to a similar definition of terrorism. Apart from the numerous conventions on terrorism to which the Philippines is party, the Philippines recently entered into an Agreement with Malaysia and Indonesia, in May 2002, to strengthen trilateral defense, border, and security cooperation. To achieve this, they undertook to cooperate among themselves in preventing the use of their territories to commit acts of terrorism.[128] The agreement substantially mirrors various existing regional multilateral conventions.[129]

It is clear from treaties, and General Assembly and Security Council resolutions that opinio juris is extant in the condemnation of all acts, methods, and practices of terrorism, wherever and whenever committed, plainly evincing that terrorism is prohibited under international law. However, while the objectives of terror-violence remain somewhat constant, namely to achieve political or power outcomes, the means by which such violence is carried out constantly evolve.[130]

How does the cyberage affect this definition? Does the phrase "all acts, methods, and practices" include all terrorist cyberactivities?

C. How Does the Cyber Age Change the Definition of Terrorism, i.e., Terrorist Attacks Through the Internet?

The Internet has provided an inexpensive mechanism,[131] free of geographical and time constraints, to distribute audio and video clips that can be

128. Agreement on Information Exchange and Establishment of Communication Procedures, Phil.-Malay.-Indon. (May 7, 2002) (on file with the Department of Interior and Local Government).

> Terrorism, which in this Agreement is understood to mean *any act of violence or threat* thereof perpetrated to carry within the respective territories of the Parties or in the border area of any of the Parties an individual or collective criminal plan with the aim of *terrorizing people or threatening to harm them or imperiling* their lives, honour freedoms, security of rights or exposing the environment or any facility or public or private property to hazards or occupying or seizing them, or endangering a natural resource, or international facilities, or threatening the stability, territorial integrity, political unity or sovereignty of independent States.

129. Convention of the Organization of the Islamic Conference on Combatting International Terrorism (Conference on Combatting International Terrorism), *adopted at* Ouagadougou on July 1, 1999, *deposited with* the Secretary-General of the League of Arab States, Annex to Resolution No. 59/26-P (1999).

130. Cherif Bassiouni, *Assessing Terrorism into the New Millennium*, 12 DEPAUL BUS. L.J. 1, 10 (2000) [hereinafter Bassiouni, *Assessing Terrorism*].

131. Schwartau, *supra* note 28, at 308-310.

extremely powerful in garnering and directing public response and action.[132] The combination of these factors makes the Internet a convenient medium of choice for terrorists.

1. The Internet

Initially developed in 1969 in the United States to facilitate the sharing of information by military researchers,[133] the Internet, called the ARPANET military program then,[134] was created to enable computers operated by the military, defense contractors, and defense-related universities to communicate by redundant channels even if an enemy attack damaged the network through nuclear attacks and atomic blasts. ARPANET epitomized the capability for developing linked non-military networks through which millions of people could communicate and access information worldwide. ARPANET was eventually renamed DARPANET, and died in 1989.[135] Other computer networks have then emerged, such as BITNET, CSNET, FIDONET and USENET, which now comprise today's Internet.

By 1999, Internet users were estimated to number around two hundred million worldwide.[136] While ARPANET began communicating through special telephone lines, modern Internet communications can travel through ordinary telephone lines, relays from microwave relay towers through the atmosphere, and satellite uplinks and downlinks.[137] The Internet has evolved

132. Edward Harris, *Web Becomes a Cybertool for Political Activists*, WALL ST. J., Aug. 5, 1999, at B11.

133. James Bussutil, *A Taste of Armageddon: The Law of Armed Conflict as Applied to Cybersim*, *in* ESSAYS IN HONOR OF IAN BROWNLIE 39 (Goodwinn-Gil ed., 1999) [hereinafter Bussutil, *A Taste of Armageddon*].

134. KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 249 (1996).

135. PRESIDENT OF THE UNITED STATES, MEMORANDUM TO SECRETARY OF DEFENSE (Sept. 29, 1999) (attaching revised Unified Command Plan ¶ 22a(12) [1999]).

136. RICHARD NEU ET AL., SENDING YOUR GOVERNMENT A MESSAGE: E-MAIL COMMUNICATION BETWEEN CITIZENS AND GOVERNMENT 119-48 (1999) [hereinafter NEU ET AL., SENDING YOUR GOVERNMENT A MESSAGE]. *See also* BRIAN NICHIPORUK & CARL H. BUILDER, INFORMATION TECHNOLOGIES AND THE FUTURE OF LAND WARFARE 34 (1995) [hereinafter NICHIPORUK & BUILDER].

137. *See generally The Internet Cuts the Cord*, WALL ST. J., Sept. 20, 1999, at A1.

enormously due to the development of transistors, microchips, and fiber optic cables.[138]

Internet access provides a myriad of communication and information retrieval methods such as electronic mail (e-mail), automatic mailing services (mail exploders), newsgroups, chat rooms, and the World Wide Web – a vast number of documents, or files containing information, stored in different computers all over the world.[139] E-mail permits the sending of an electronic message to another party or a group of addressees. The message is stored electronically, awaiting a recipient's checking his or her "mailbox" or making its presence known through a prompt signal. Unlike postal mail, e-mail usually is not sealed or secure.[140] It can be accessed or viewed on intermediate computers between sender and recipient, unless messages are encrypted.[141] Further, it is possible to send messages to a common e-mail address, which then forwards them to other subscribers, through what is known as mail exploders.[142] All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium – known to its users as "cyberspace" – located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.[143]

2. The Crime of Hacking

To date, web hacks and computer break-ins, whether against commercial or governmental computers, are extremely common. Reports have revealed that certain groups from Russia and Bulgaria,[144] or the Zapatista indigenous group in Mexico,[145] have utilized the Internet to express their views and take action. Organizations such as the Italian Mafia, Columbian drug cartels,

138. NICHIPORUK & BUILDER, INFORMATION TECHNOLOGIES, *supra* note 136, at 8-10, 14-15.

139. *See* Tim Berners-Lee et al., *The World Wide Web, in* COMMUNICATIONS OF THE ACM 76-82 (1994).

140. NEU, SENDING YOUR GOVERNMENT A MESSAGE, *supra* note 136, at 95-177.

141. *See generally* Wayne Madsen et al., *Cryptography and Liberty: An International Survey of Encryption Policy*, 16 J. MARSHALL J. COMPUTER & INFO. L. 475 (1998).

142. NEU, SENDING YOUR GOVERNMENT A MESSAGE, *supra* note 136, at 149-51.

143. Reno v. ACLU, 521 U.S. 844, 851 (1997).

144. A. Rathnell, Cyberwar, *The Coming Threat, National Criminal Intelligence Service Pointer, at* www.kcl.ac.uk/orgs/icsa/ncis.htm (last visited Jan. 3, 2002).

145. For an extensive analysis of the Zapatista's netwar, *see* RONFELDT ET AL., THE ZAPATISTA SOCIAL NETWAR IN MEXICO, RAND REPORT MR-994-A (1998) [hereinafter RONFELDT ET AL., THE ZAPATISTA].

and Russian organized crime groups have even hired skilled hackers to enable them to profit more lucratively.[146]

Terrorist groups also use the Internet extensively to spread their message and to communicate and coordinate action.[147] They provide a forum for their own agenda by publishing their works and ideology.[148] In fact, some hackers suspected of being terrorists publish electronic magazines and put up Web sites with software tools and information about hacking,[149] including details about vulnerabilities in popular systems and how they can be exploited, programs for cracking passwords, software packages for writing computer viruses, and scripts for disabling or breaking into computer networks and Web sites.[150] In 1997, an article in the New York Times reported that there were an estimated 1,900 Web sites purveying hacking tips and tools, and 30 hacker publications.[151] Subsequently, the U.S. News & World Report noted that 12 of the 30 groups on the U.S. State Department's list of terrorist organizations are on the Web.[152]

With the ease and convenience of the Internet, it has introduced varying degrees of computer misuse, originally domestic in nature,[153] and eventually transcended national boundaries with the merger of computer and communications technologies permitting a user located in one State to access computer systems almost anywhere in the world.[154] It has facilitated

146. Joshua Cooper Ramo, *Crime Online: Mobsters Around the World Are Wiring for the Future*, TIME, Sept. 23, 1996, at TD32.

147. COMMUNIQUE, MEETING OF THE JUSTICE AND INTERIOR MINISTERS OF THE EIGHT (1997).

148. Braun et al., *WWW.COMMERCIAL_TERRORISM: A Proposed Federal Criminal Statute Addressing the Solicitation of Commercial Terrorism Through the Internet*, 37 HARVARD J. LEG. 159, 160 (2000).

149. George du Pont, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. TECH. L. REV. 191, 191 (2000/2001) [hereinafter Du Pont, *The Criminalization*].

150. RONFELDT ET AL., THE ZAPATISTA , *supra* note 145, at 66.

151. *See* Steve Lohr, *Go Ahead, Be Paranoid: Hackers Are out to Get You*, N.Y. TIMES, Mar. 17, 1997.

152. Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Feb. 4, 2000, *at* http://www.nautilus.org/info-policy/workshop/papers/denning.html. (last visited May 30, 2002) [hereinafter Denning, *Activism, Hacktivism, and Cyberterrorism*].

153. COMPUTER LAW, *supra* note 24, at 242 (revealing that the European Community, Austria, France, Denmark, Finland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, and West Germany enacted computer crime statutes even during the 1980s).

154. *Id.* at 242.

transnational terrorism, particularly cyberterrorism, [155] sometimes even through cybermercenaries.[156] National governments experience less control over currencies and their valuation, markets and prices, businesses and their regulation, national borders and people and commodity movements across them, and information available to the public.[157] Consequently, States have increasingly found their powers curtailed by the accessibility of information systems to cybercriminals.[158]

These international aspects of cybercriminality have prompted the involvement of agencies such as the Organization for Economic Cooperation and Development, [159] the International Chamber of Commerce,[160] the Council of Europe,[161] the Ministers of The Eight,[162] and the United Nations[163] in an ongoing debate about the need for and form of an international action plan.

155. NICHIPORUK & BUILDER, *supra* note 136, at 32-35 Carl H. Builder, *The American Military Enterprise in the Information Age, in* STRATEGIC APPRAISAL: THE CHANGING ROLE OF INFORMATION IN WARFARE 19, 31 (Zalmay M. Khalilzad & John P. White eds., 1999) [hereinafter Builder, *The American Military Enterprise*]; Jessica Mathews, *Power Shift*, FOREIGN AFFAIRS, Jan.-Feb. 1997, at 50-1 [hereinafter Mathews].

156. Glenn C. Buchan, *Implications of Information Vulnerabilities for Military Operations, in* STRATEGIC APPRAISAL: THE CHANGING ROLE OF INFORMATION IN WARFARE 283, 314 (Zalmay M. Khalilzad & John P. White eds., 1999).

157. NICHIPORUK & BUILDER, *supra* note 136, at 35-38; Alvin Toffler & Heidi Toffler, *Foreword, in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE xiii, xiv-xvi (John Arquilla & David Ronfeldt eds., 1997).

158. *See* THE THIRD WAVE, *supra* note 3, at 325; Builder, *The American Military Enterprise, supra* note 155, at 25-26.

159. O.E.C.D. REPORT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980); O.E.C.D. REPORT, COMPUTER RELATED CRIME: ANALYSIS OF LEGAL POLICY (1986); INTERNATIONAL CHAMBER OF COMMERCE REPORT, ALLIANCE AGAINST COMMERCIAL CYBERCRIME (1999).

160. INTERNATIONAL CHAMBER OF COMMERCE, COMMISSION ON COMPUTING, TELECOMMUNICATIONS AND INFORMATION POLICIES, COMPUTER-RELATED CRIME: AN INTERNATIONAL BUSINESS VIEW (1988).

161. European Council Directive on the Protection of Individuals with regard to the Processing of Data and on the Free Movement of such Data, E.C. Directive/95/46 (1995); FINAL ACTIVITY REPORT, COMMITTEE OF EXPERTS ON CRIME IN CYBERSPACE (2001).

162. MEETING OF THE EIGHT, 10 PRINCIPLES AND ACTION POINTS (1997).

163. G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc.A/RES/53/70 (1998).

But does computer use per se by terrorist groups constitute terrorism? Is the mere posting of terrorist sites cyberterrorism in itself?

Increasingly hostile activities on the Internet[164] warrant the conclusion that disruptive cyberattacks[165] will take center stage in the future.[166] It is not surprising that the resources needed to launch these attacks are commonplace in the world,[167] as a computer and a connection to the Internet are all that are really needed to wreak havoc against a State's critical networks.[168] Nonetheless, every activity by terrorists over the Internet should not constitute cyberterrorism; otherwise each hacking activity by alleged terrorists would qualify as such.[169] As thousands of persons[170] and groups[171] around the world engage in intrusive or disruptive cyberactivities,[172] every cyberattack should not readily[173] be characterized as cyberterrorism. The real terror-generating cyberactivity refers to serious cyberattacks [174] against networks controlling electricity, communications and computer systems

164. Gene Barton, *Taking a Byte Out of Crime: E-Mail Harassment and the Inefficacy of Existing Law*, 70 WASH. L. REV. 465, 471 (1995).

165. FORESTER AND MORRISON, COMPUTER ETHICS: CAUTIONARY TALES AND ETHICAL DILEMMAS IN COMPUTING 49-50 (1990).

166. MANN, COMPUTER TECHNOLOGY AND THE LAW IN CANADA 171 (1987). *See also* Schwartz, *Hackers of the World*, NEWSWEEK, Jul. 2, 1990, at 36.

167. NICHIPORUK & BUILDER, *supra* note 136, at 34.

168. *See* ROBERT ANDERSON ET AL., SECURING THE U.S. DEFENSE INFORMATION INFRASTRUCTURE: A PROPOSED APPROACH 1-3 (1999). *See also* Michael Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 YALE HUM. RTS. DEV. L.J. 143, 164 (1999) [hereinafter Schmitt].

169. *Hearings by the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee* , 105th Cong. (1998) (testimony of Clark L. Staten).

170. L. Warrior, The Information Warriors, *Defence Systems International 98, at* www.kcl.ac.uk/orgs/icsa/warrior2.htm. (last visited May 30, 2002).

171. A. Rathnell et al., *The IW Threat from Sub-State Groups: an Interdisciplinary Approach* (Jun. 1997), *at* www.kcl.ac.uk/orgs/icsa/terrori.html (last visited May 28, 2002).

172. Chaos Computer Club, *available at* www.ccc.de; !Hispahack, *available at* www.hispahack.cc.de; Phrack, *available at* www.phrack.com; Pulhas, *available at* www.p.ulh.as/; Toxyn, *available at* www.toxyn.org. These sites portray and expose hacking techniques.

173. Associated Press, *Beijing Tries to Hack U.S. Web Sites*, Jul. 30, 1999, *available online at* www.falunusa.net. (last visited Apr. 30, 2002).

174. *Americans Addiction to Computers May Leave U.S. Open to Terror Attacks*, WINSTON-SALEM J., Nov. 5, 1999, at A14.

necessary to the survival of a State,[175] ultimately affecting the civilian population.

What then constitutes cyberterrorism?

II. ASCERTAINING *OPINIO JURIS* AND EVALUATING STATE PRACTICE IN THE LEGAL CHARACTERIZATION AND DEFINITION OF *CYBERTERRORISM*: TERRORISM IN A NEW MEDIUM

As of 15 December 2003, the 12th Philippine Congress has not yet passed a bill on cyberterrorism; in fact, not even a bill on terrorism. It is interesting to note, however, that Representative Imee Marcos proposed House Bill 3802[176] defining and penalizing cyberterrorism, among other crimes, in recognition of the fact that the Philippines has become an arena of terrorism. The bill was designed to improve the substantive provisions of Philippine penal law to directly address all methods of terrorism, including the movement of suspected foreign terrorists and their various support resources into the country.[177] It defines cyberterrorism as:

> [U]nauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents.[178]

Is this definition consistent with current International Law norms defining cyberterrorism? It would seem that the definition is overbroad. Although the opinio juris of States regards terrorism in any manner and

175. Note, *Discrimination in the Laws of Information Warfare*, 37 COLUM. J. TRANSNAT'L L. 939, 940 (1999).

176. H.B. 3802, An Act Defining Terrorism, Providing Penalties Therefor and For Other Purposes, 12th Cong. (1st Regular Sess. 2001). The author likewise conducted an interview with the staff of Congressman Marcos to further elucidate the matter.

177. As of March 1, 2003, the Bill was still pending before the House Committee on Justice. The Committee consolidated the bill with two other new bills: House Bill 4980 and House Bill 5025. Unlike House Bill 3802, these latter bills did not define cyberterrorism but instead subsumed cyberterrorism under the general crime of terrorism. It must be noted also that an Inter-agency Draft, dated July 9, 2002, was drawn by certain governmental instrumentalities.

178. *Id.* § 3(i).

however committed as outlawed,[179] State practice has shown that not all cyberactivities by terrorists should be deemed cyberterrorism.

How should the Philippines define cyberterrorism?

For this purpose, State practice[180] and opinio juris,[181] shall be extensively analyzed by the author. Since State practice does not only consist of what States do but also what they say,[182] it may also be observed from a pattern of treaties in the same form[183] if coupled with a degree of repetition over a period of time,[184] and from the practice of international organs.[185] As to the element of opinio juris, the International Court of Justice (ICJ) has been willing to assume its existence on the bases of evidence of a general practice or a consensus in the literature, or the previous determination of the Court or other international tribunals.[186] In this respect, recent legislation has been enacted by various States with respect to cybercrimes. In addition, acts of international organs have been recently accorded a special role in determining new norms of international law.[187] Imperatively, as rules

179. *See supra* notes 81-84.

180. Continental Shelf Case (Libya v. Malta), 1985 I.C.J. 29, ¶¶ 27-34. State practice may be either actual or behavioral. *See* D'AMATO, CONCEPT OF CUSTOM IN INTERNATIONAL LAW 88 (1971) (explaining that State practice is actual when it relates to physical acts); VILLEGER, CUSTOMARY INTERNATIONAL LAW AND TREATIES 4 (1985) (discussing that it is behavioral when it refers to any act or statement by a State showing a conscious attitude to recognize it as binding unto itself).

181. LAUTERPACHT, THE DEVELOPMENT OF INTERNATIONAL LAW BY THE INTERNATIONAL COURT 380 (1958) [hereinafter LAUTERPACHT]; HARRIS, *supra* note 1, at 41 ("*Opinio juris* then is the psychological element of a custom, the belief that a particular State Practice is binding, which differentiates a custom from mere comity."); North Sea Continental Shelf Case (Germany v. Denmark) (Germany v. Netherlands), 1968 I.C.J. 3 (pointing out that State practice must be carried out in such a way as to evidence a belief that this practice is rendered obligatory by the existence of a rule of law requiring it).

182. AKEHURST'S MODERN INTRODUCTION TO INTERNATIONAL LAW 43 (Peter Malanczuk ed., 1997) [hereinafter AKEHURST'S MODERN INTRODUCTION].

183. Delimitation of the Maritime Boundary in the Gulf of Maine Area, 1982 I.C.J. 294, ¶¶ 94-96.

184. Asylum Case (Columbia v. Peru), 1950 I.C.J. 277.

185. *See* Genocide Case (Bosnia & Herzegovina v. Yugoslavia), 1951 I.C.J. 25.

186. IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 7 (1990) [hereinafter BROWNLINE, INTERNATIONAL LAW]; LAUTERPACHT, *supra* note 181, at 380; *Gulf of Maine*, 1982 I.C.J. 294.

187. Skubiszweski, *Resolutions of the UN General Assembly and Evidence of Custom*, *in* 1 ETUDES EN I'HONNEUR DE R. AGO 503 (1987); J.A. Frowein, *The Internal and*

governing cyberattacks are at their nascent stage, these sources provide a skeleton for the author's attempt in delineating the appropriate definition of, and responses to, cyberattacks.

More importantly, and as previously mentioned, resolutions of the United Nations General Assembly, even if not binding per se, sometimes have normative value as they, in certain circumstances, provide evidence important for establishing the existence of a rule or the emergence of opinio juris.[188] Further, these Resolutions contribute to customary international law as a form of collective State practice[189] – a somewhat collective equivalent of unilateral general statements.[190] For instance, a resolution of the General Assembly can be evidence of customary law because it reflects the views of the States voting for it.[191]

Since the opinio juris regarding the prohibition of all methods and practices of terrorism seems to be clear,[192] it is the element of State practice relating to cyberterrorism that shall be primarily paid attention to by the author.

A. G.A. Resolution 53/70[193] *and Cyberterrorism*

At the initiative of the Russian Federation, the U.N. General Assembly, in December 1998, adopted a Resolution related to cybercrime, cyberterrorism, and cyberwarfare. Resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security, provides, in pertinent part:

> The General Assembly,
>
> x x x[*]

External Effects of Resolutions by International Organizations, 49 Z.A.O.R.V. 778-90 (1989).

188. Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, *reprinted in* 35 I.L.M. 809 & 1343 (1997). *See generally* S. Schwebel, *The Effect of Resolutions of the UN General Assembly on Customary International Law*, *in* PROCEEDINGS OF THE ASIL 301 (1979); G. Arango-Ruiz, *The Normative Role of the General Assembly of the United Nations and the Development of Principles of Friendly Relations*, III RECUEIL DES COURS 431 (1972).

189. HARRIS, CASES AND MATERIALS, *supra* note 1, at 61.

190. Truman Proclamation on the Continental Shelf Case, *cited in* HARRIS, CASES AND MATERIALS, *supra* note 1, at 61.

191. AKEHURST'S MODERN INTRODUCTION, *supra* note 182, at 52.

192. *See infra* discussion on Part II.

193. G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc.A/RES/53/70 (1998).

> Calls upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;
>
> 2. Invites all Member States to inform the Secretary-General of their views and assessments on the following questions:
>
> (a) General appreciation of the issues of information security;
>
> (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;
>
> (c) Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.[194]

It must be noted, however, that G.A. Resolution 53/70, when tested under the Namibia[195] or Western Sahara Case,[196] may not be adjudged as law in itself[197] as no legal obligation is imposed on States,[198] except that of extending information.[199] It is not declaratory of international law because it appears to concern itself with recommendatory or procedural powers, rather than with general international law.[200] In fact, the tenor of said G.A. Resolution is not in itself mandatory, but hortatory,[201] and does not define cyberterrorism. Nevertheless, it is a first step in the process of law creation.[202] Although opinio juris as to the illegality of cyberterrorism may be deduced from the text of G.A. Resolution 53/70, how does State practice supply the other element in defining cyberterrorism? Thus, an attempt to define cyberterrorism based on State practice seems essential.

To arrive at a universally acceptable definition of cyberterrorism, evidence should be sought in the behavior of the great majority of interested States, in this case, technologically-advanced States who have identified

194. *Id.* (italics supplied).

195. *Namibia*, 1971 I.C.J. at 16.

196. *Western Sahara*, 1975 I.C.J. at 12.

197. GAETANO ARANIO RUIZ, THE UNITED NATIONS DECLARATION ON FRIENDLY RELATIONS AND THE SYSTEM OF THE SOURCES OF INTERNATIONAL LAW 85 (1979).

198. OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 85 (1995).

199. G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc.A/RES/53/70 (1998).

200. ROSALYNN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 26 (1994) [hereinafter HIGGINS, PROBLEMS AND PROCESSES].

201. *See* HARRIS, CASES AND MATERIALS, *supra* note 1, at 59 (discussing such kinds of G.A. Resolutions).

202. Declarations of the United Kingdom, Mexico and Iraq, *supra* note 83.

critical infrastructure, as how the World Court was called to do in the past in the North Sea Continental Shelf Case:

> Finally, it is noteworthy that about seventy States are at present engaged in the exploration and exploitation of continental shelf areas...
>
> For to become binding, a rule or principle of international law need not pass the test of universal acceptance. This is reflected in several statements of the Court, *e.g.* "generally...adopted in the practice of States. Not all States have an opportunity or possibility of applying a given rule. The evidence should be sought in the behavior of a great number of States, possibly the majority of States, in any case the great majority of the interested States...."[203]

Only substantial, not complete, uniformity in State practice is required, as held in the Anglo-Norwegian Fisheries Case.[204] State practice may be observed from municipal legislations and proceedings, statements by national legal advisers in domestic and international fora[205] – as indorsed by Judge Ammoun in his Dissenting Opinion in the Barcelona Traction Case[206] – likewise from policy statements or press releases of States.[207] Inconsistency per se of such behavior, unless too uncertain and influenced by political expediency,[208] would not prevent a definition from being concluded, for as long as these inconsistencies may be analyzed, the author may detect the least common denominator among all the views and practices of these States.[209]

B. State Practice and Cyberterrorism

The main impact of cyberthreats on foreign and domestic policy relates to defending against such acts, particularly attacks against critical infrastructure,[210] as can be apparently gathered from the practice of States.

203. *See North Sea*, 1969 I.C.J. at 3 (Lachs, J., dissenting) (citing Fisheries Judgment, 1951 I.C.J. 128)

204. Anglo-Norwegian Fisheries (U.K. v. Norway), 1951 I.C.J. 191.

205. REBECCA WALLACE, INTERNATIONAL LAW 15 (3d. 1997) [hereinafter WALLACE].

206. Barcelona Traction, light and Power Company (Belgium v. Spain), 1970 I.C.J. 3 (Ammoun, J., dissenting).

207. BROWNLIE, INTERNATIONAL LAW, *supra* note 186, at 4; HARRIS, CASES AND MATERIALS, *supra* note 1, at 26.

208. *Asylum Case*, 1950 I.C.J. 266.

209. WALLACE, *supra* note 205, at 11.

210. Yonah Alexander, *Terrorism in the Twenty-First Century: Threats and Responses*, 12 DEPAUL BUS. L.J. 59, 89 (2000) [hereinafter Alexander, *Terrorism*].

Several countries, especially the U.S.,[211] have addressed such issues through mutual legal assistance treaties, extradition, sharing of intelligence, and continuing conferences on the need for uniform computer crime laws so that cyberterrorists can be successfully investigated and prosecuted when their crimes cross international borders. In recent years, data protection has come under active consideration[212] in most of the technologically-advanced States, such as the United Kingdom, the United States, Austria, France, Denmark, Finland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, and West Germany.[213]

The contemporary origins of the issue began when President Clinton signed Presidential Decision Directive 39 ("PDD-39"), tasking the Attorney General with examining how the United States had become more vulnerable to physical attacks, particularly in the wake of the 1993 bombings at the World Trade Center in New York, and the Alfred P. Murray Building in Oklahoma City.[214] At the same time, the national security community realized that the U.S. was becoming more vulnerable to electronic attacks.[215] The Attorney General then convened the Critical Infrastructure Working Group ("CIWG") to examine these issues, which, in turn, recommended the creation of a commission to study both physical and cyber vulnerability issues, emphasizing how the two might represent a tandem threat.[216]

Based on that recommendation, the President signed Executive Order 13010 on 15 July 1996 establishing the President's Commission on Critical Infrastructure Protection (PCCIP).[217] After a year of deliberations, the PCCIP submitted its final report to the President in October 1997, which prompted the President to sign the Presidential Decision Directive 63 (PDD-

211. Aldrich, *War in the Information Age*, *supra* note 44, at 260. *See Hearings before the House Joint Committee on Preventing Economic Cyber Threats* (Feb. 23, 2000) (testimony of John A. Serabian Jr.) [hereinafter *Hearings before the House*].

212. COMPUTER LAW, *supra* note 24, at 242.

213. *See generally* Jessica McCausland, *Regulating Computer Crime After* Reno v. ACLU: *The Myth of Additional Regulation*, 49 FLA. L. REV 483, 501 (1997) [hereinafter McCausland, *Regulating Computer Crime*].

214. REPORT OF THE PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURE 5 (1997) [hereinafter PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION].

215. Frank J. Cilluffo et al., *Bad Guys and Good Stuff: When and Where Will the Cyber Threats Converge?* 12 DEPAUL BUS. L.J. 131, 134 (2000).

216. INTERNAL MEMORANDUM FROM THE CRITICAL INFRASTRUCTURE WORKING GROUP ("CIWG") (1996).

217. Exec. Order No. 13010, 61 Fed. Reg. 37, 347 (1996).

63), representing the federal government's current official policies on matters of critical infrastructure assurance.[218]

In December 2000, the U.S. national domestic terrorism advisory panel released its second annual report on terrorism, weapons of mass destruction, and cyberterrorism, in which they stated,

> [T]hat it was easy to envision a coordinated attack *by terrorists*, using a conventional or small-scale chemical device, with simultaneous *cyber attacks against law enforcement communications, emergency medical facilities, and other systems critical to respond to the non-cyberattack.*[219]

Accordingly, U.S. advisers describe cyberterrorism as cyberattacks that would disrupt banks, international financial transactions and stock exchanges, gain entry to the Federal Reserve building, attack air traffic control systems, crack the aircraft's in-cockpit sensors, or alter the formulas of medication at pharmaceutical manufacturers.[220]

In the same fashion, Japan has taken certain significant policy steps against cyberterrorism. The Japanese Government, as a member of The Eight, has reserved $1.4 billion of its budget to fight cyberterrorism, and has adopted a law that would make it a crime to damage computer networks of companies, government offices, universities and others entered through the use of stolen IDs or holes in network defenses.[221] A National Police Agency was created to serve as a high-tech anti-cybercrime investigative and analysis center, and a Commission on Critical Infrastructure Protection was established in September 1998.[222]

Similarly, the European Community has condemned cyberspace offenses committed against the integrity, availability, and confidentiality of communications systems and telecommunications networks, resulting in

218. *See Protecting America's Infrastructure*, PDD WHITE HOUSE FACT SHEET (May 22, 1998).

219. U.S. ADVISORY PANEL REPORTS ON CYBERTERRORISM (2000) (emphasis supplied).

220. Barry C. Collin, Remarks during the 11th Annual International Symposium on Criminal Justice Issues, The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge (1996) [hereinafter Collins, Remarks].

221. Raisuke Miyawaki, Speech before the Center for Strategic & International Studies (Jun. 29, 1999) [hereinafter Miyawaki].

222. *Id.* Similar to that of the U.S., the Commission consists of the heads of Japan's top infrastructure firms, and a former Deputy Chief Cabinet Secretary. It was formed specifically to make Japan's industry aware of its need for measures to protect network and infrastructure lifelines against cyberattacks. In 1999, it began efforts to develop and promote Japan-US cooperation on critical infrastructure protection.

coercion, illegal money transactions, and violation of human dignity.[223] On 6 January 2001, the European Commission issued a communication to the Council, the European Parliament, the Economic and Social Committee, and the Committee of the Regions, entitled "Creating a Safer Information Society by Improving the Security of Information Infrastructure and Combating Computer-related Crimes."[224] The Communication addressed such topics as threats, substantive and procedural law issues (e.g., interception of communications, retention of traffic data, anonymous access and use, practical co-operation at international level), and jurisdictional issues, and proposed both legislative and non-legislative measures as responses to cybercrime.[225] The United Kingdom (U.K.) leads the battle against cybercrime as they have already launched their first national law enforcement organization dedicated to fighting Internet-related crime.[226] The special police force, named the National Hi-Tech Crime Unit, consists of 80 law enforcement specialists who will be based throughout the country to assist local police force to detect and investigate such crimes.

On the international plane, the International Chamber of Commerce (ICC), whose policies are adopted by the respective national authorities due to their rational economic sense,[227] has called upon governmental authorities to pursue cybercriminals who have targeted critical infrastructure on which communities depend, e.g. telecommunications, banking and finance, energy, transportation and government services.[228] The ICC appealed to authorities around the world to cooperate in fighting cybercrime by emphasizing that critical infrastructure require protection through the joint commitment of the public and private sectors.

223. *See* DRAFT EXPLANATORY REPORT, DRAFT CONVENTION ON CYBER-CRIME AND EXPLANATORY MEMORANDUM RELATED THERETO (2001).

224. *Creating a Safer Information Society by Improving the Security of Information Infrastructure and Combating Computer-related Crime, Communication of the European Commission*, COM (2000) 890, *available at* http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm (last visited Jun. 5, 2002).

225. *See Network and Information Security: Proposal for a European Policy Approach, Communication of the European Commission*, COM(2001)298, *at* http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm (last visited May 29, 2002).

226. *U.K. Launches CyberPolice, available at* http://www. cnn.com (last visited Jul. 11, 2002).

227. *See generally* CONFERENCE REPORT, ALLIANCE AGAINST COMMERCIAL CYBERCRIME (1999).

228. INTERNATIONAL CHAMBER OF COMMERCE, COMMISSION ON COMPUTING, TELECOMMUNICATIONS AND INFORMATION POLICIES, COMPUTER-RELATED CRIME: AN INTERNATIONAL BUSINESS VIEW (1988).

The Eight, which is composed of the G-7 members (England, Italy, France, Germany, Japan, Canada, and the U.S.) and Russia,[229] has also summoned the whole international community to take action plans against terrorists using and targeting computer systems, posing serious threats to public safety, to facilitate their violent activities.[230] The G-8 communiqué recognized the urgent need to make rapid progress in these areas and announced that it would take the steps necessary to ensure protection from the physical and financial predation of transnational organized crime, although the task would be daunting.

It appears from the actions taken by the States that while the cyberage has changed the medium of attack by a terrorist,[231] the same elements found in traditional terrorism should still apply, [232] except that there are cyberterrorist attacks when no violence results but severe economic hardship[233] since there are computer systems that are not concerned with public safety but with public welfare.[234] Public safety would be involved in a cyberterrorist attack against transportation systems and hospital life support systems, while public welfare would relate to a cyberterrorist attack resulting in destruction or suspension of vital services upon which civilian functions depend, such as power plants, or banks and stock exchange centers.[235]

These actions have received insignificant protest from organizations, and even States from which protest could be expected, such as the members of the Organization of the Islamic Conference, who have included in their definition of terrorism any act of violence or threat thereof exposing the environment or any facility or public or private property to hazards or occupying or seizing them, or endangering a national resource, or international facilities.[236] In the same vein, the League of Arab States has recognized that any act or threat of violence in the advancement of an individual or collective criminal agenda causing fear by seeking to cause damage to the environment or to public or private installations or property

229. *Cybercrimes*, 3 CYBERSPACE L. 32 (1998).

230. COMMUNIQUE, MEETING OF THE JUSTICE AND INTERIOR MINISTERS OF THE EIGHT (1997).

231. Mathews, *Power Shift*, *supra* note 155, at 51. *See* REPORT OF THE EUROPEAN COMMITTEE ON CRIME PROBLEMS, CDPC/103/211196 (Nov. 1996).

232. BARRY COLIN, THE FUTURE OF CYBERTERRORISM, CRIME AND JUSTICE INTERNATIONAL 15-8 (1997).

233. Sproles & Byars, *supra* note 29.

234. Graham, *supra* note 29.

235. Nigel Thompson, *Internet Crime*, *in* TERRORISM AND INTERNET WARFARE 4 (1998) [hereinafter Thompson, *Internet Crime*].

236. Conference on Combatting International Terrorism, *supra* note 129.

or to occupying or seizing them, or seeking to jeopardize a national resources, is a terrorist act.[237]

C. Defining Cyberterrorism

Prescinding from these actions taken both on the municipal and international levels, cyberterrorism can be defined as the politically motivated attack, through the use of computers and against computers controlling critical infrastructure,[238] resulting in violence[239] or serious economic hardship to civilians or non-combatants,[240] generating a state of terror in the minds of the general public.[241]

By this definition, it appears that House Bill 3802, proposed by Representative Imee Marcos, does not comply with the norms followed by States. To be classified as cyberterrorism, the act must consist of a computer-generated attack against computer systems of adverse entities, whether civilian, corporate, or governmental, which affect personal lives and impacts on national and international security.[242] Terrorist computer "hackers" achieve their goals by destroying secure computer files and database entries in order to cause damage to their targets as a consequence.[243]

As not all cyberactivities of terrorists should be deemed cyberterrorism, the term must be understood to mean a computer-based attack intended to intimidate or coerce governments or societies in pursuit of goals that are political or ideological, and sufficiently destructive or disruptive to generate

237. Arab Convention for the Suppression of Terrorism, Adopted by the Council of Arab Ministers of the Interior and the Council of Arab Ministers of Justice at Cairo, Egypt (Apr. 1998) *available at* http://www.lasmediaservice.htm (last visited Jul. 14, 2002)

238. Alexander, *Terrorism*, *supra* note 210, at 72.

239. *Compare* Pollitt, *Fact or Fancy?*, *supra* note 33, at 285-9, *with* Kevin Soo Hoo et al., *Information Technology and the Terrorist Threat*, 39 SURVIVAL 135-55 (1997) [hereinafter Hoo].

240. For a thorough discussion on how a cyberterrorist attack may cause serious economic hardship, *see* CYBER TERRORISM AND INFORMATION WARFARE: THREATS AND RESPONSES (Yonah Alexander & Michael S. Swetman eds., 1999).

241. *Hearings before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives*, 107th Cong. (May 23, 2000).

242. Pollitt, *Fact or Fancy?*, *supra* note 33.

243. *See* Bassiouni, *Assessing Terrorism*, *supra* note 130, at 14. Cyberterrorists destroy corporate computer files, access private database entries, falsely manipulate the stock market, reroute transportation systems, intercept military communications, disrupt banking operations, and manipulate government files.

fear comparable to physical acts of terrorism.[244] The impact of these acts, while materially different from traditional attacks, such as bombing or assassinations, are capable of generating higher levels of insecurity and likely a more harmful impact on society.[245]

D. Elements of Cyberterrorism

1. First Element: The cyberattack must be against critical infrastructure computer systems causing severe harm or violence to civilians.

Cyberterrorist acts are computer attacks against critical infrastructure systems[246] harming non-combatants, or the civilian segment of the population.[247] The immediate target of cyberterrorists is the infrastructure system;[248] the real target, however, being innocent third parties.[249] The targeting of civilians is symbolic: the act of harming civilians is neither legally nor morally justifiable despite any perceived goodness of the goal sought,[250] since such act is not likely to give terrorists the public support for their political aims.[251]

a.) What Qualify as Critical Infrastructure?

Critical infrastructures are those national systems so vital to the State that their incapacity or destruction would have a debilitating impact on the defense or economic security of the State.[252] The U.S. has classified eight categories of critical infrastructure, which include: telecommunications, transportation, electric power systems, banking and finance, water supply systems, gas and oil storage and transportation, emergency services (medical,

244. Denning, *Is Cyber Terror Next*, *supra* note 12.

245. Bassiouni, *Assessing Terrorism*, *supra* note 130, at 14.

246. *See generally* Hoo, *supra* note 240.

247. *See* FBI Denver Division, *International Terrorism*, *available at* http://www.fbi.gov/contact/fo/denver/inteterr.htm (last visited May 14, 2001).

248. Denning, *Is Cyber Terror Next*, *supra* note 12.

249. RICHARD LILICH, TRANSNATIONAL TERRORISM: CONVENTIONS AND COMMENTARY 199 (1982).

250. *See generally* K. Greene, *Terrorism as Impermissible Political Violence: An International Law Perspective*, 16 VT. L. REV. 461, 476-7 (1992); L. Goldie, *Profile of a Terrorist: Distinguishing Freedom fighters from Terrorists*, 14 SYR. J. INT'L L. & COM. 125 (1987).

251. Bassiouni, *Assessing Terrorism*, *supra* note 130, at 10.

252. U.S. Exec. Order No. 13,010, 61 Fed. Reg. 37347 (1996).

police, fire and rescue), and other infrastructure relating to the continuity of government[253] for the benefit of the civilian population.

b.) Why Critical Infrastructure?

Computer controlled critical infrastructure are closely intertwined with civilian life.[254] Computers speed up attacks against critical infrastructure, thus providing greater exposure of persons and property, and more opportunities for such terrorists to cause violence or serious harm.[255] Governmental and societal fear is thus enhanced by cyberthreats against national infrastructure, public and private buildings, and transportation systems. Indeed, attacks upon power plants, water and sewage filtration centers, and communications networks have the potential to cause large-scale damage and havoc to civil society, creating significant physical, environmental, and economic damage.[256] Attacks against the financial infrastructure would erode the capacity of business to function normally and raise questions among the terrified public about the security of their personal finances.[257] Clear examples of cyberterrorist actions include hacking into an air traffic control system that results in planes colliding, or attacking a stock exchange's computer systems leading to a stock market crash,[258] since both actions have far-reaching, chilling effects on an entire society.

253. *See* ROBERT T. MARSH, U.S. COMMISSION ON CRITICAL INFRASTRUCTURE INFORMATION REPORT (1997). *See also* U.S. Presidential Decision Directives (PDD) 62 & 63 (1998); Richard Clarke, *Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks*, 12 DEPAUL BUS. L.J. 33, 36 (2000).

254. *See* SECOND ANNUAL REPORT OF THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION (Dec. 15, 2000).

255. Nicolas Laos, *Information Warfare and Low Intensity Operations*, 4 PERCEPTIONS 174 (1999).

256. *See generally* Herbert H. Brown, *Nuclear Facilities and Materials*, *in* LEGAL ASPECTS OF INTERNATIONAL TERRORISM 149 (Alona Evans & John Murphy eds., 1978) [hereinafter LEGAL ASPECTS]; Brian M. Jenkins & Alfred P. Rubin, *New Vulnerabilities and the Acquisition of New Weapons by Non-government Groups*, *in* LEGAL ASPECTS, *supra*.

257. *Combating Security Threats*, NATO REV. 18 (2001).

258. BARRY COLLIN, THE FUTURE OF CYBERTERRORISM 15-18 (1997) [hereinafter COLLINS, THE FUTURE].

2. Second Element: It must be politically[259] motivated.

Just as terrorism is played before an audience in the hope of creating a mood of fear for political purposes,[260] cyberterrorism is the politically motivated use of hacking techniques in an effort to cause grave harm, including loss of life or serious economic damage.[261] The political aspect of any terrorist act means that the intimidation of a governing authority is the objective, accomplished by the attack against the community of civilians governed.[262] While recent events have called for the removal of the political motive as an element in a terrorist act, the greater weight of authority adheres to its inclusion. The political motive must be present; otherwise, such a cyberattack may simply be qualified as some other crime.

a.) The political motive may be proclaimed or gathered.

While motive is generally not essential to prove a crime, this is not so when it is an essential element of the crime.[263] The political motive of a cyberterrorist[264] may either be express, or presumed.

i.) The cyberterrorist almost always proclaims his motive.

Cyberterrorists execute their activities frequently by an explicit political expression attached to the mode of attack. This purposeful self-exposure brings to light the personality of the perpetrator,[265] which could clearly reflect his motive.[266] Usually, it takes the form of a political message

259. The word "political" has been taken to include ideological or religious belief. *See* BLAKESLEY, TERRORISM, *supra* note 124, at 40.

260. WHITE J.R., TERRORISM: AN INTRODUCTION 5-8 (1991); US. DEPARTMENT, PATTERNS OF GLOBAL TERRORISM 1992 v (1993); CINDY COMBS, TERRORISM IN THE TWENTY-FIRST CENTURY 8 (1997).

261. COLLIN, THE FUTURE, *supra* note 259.

262. *Criminology of Terrorism*, *available at* http://www.faculty.ncwc.edu/toconnor/415/415lects.htm (last visited Jul. 12, 2002) [hereinafter *Criminology of Terrorism*].

263. Adam Candeub, *Motive Crimes and Other Minds*, 142 UNIV. PENN. L. REV. 2071, 2104 (1984).

264. Pollitt, *Fact or Fancy?*, *supra* note 33.

265. Du Pont, *The Criminalization*, *supra* note 149, at 191.

266. Denning, *Activism, Hacktivism, and Cyberterrorism*, *supra* note 152. Professor Denning provides the following examples of such motives:

1.) In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP and damaged part of the ISP's record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

2.) In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the Webs site for the Euskal Herria Journal, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the 'mail bombings.'

3.) In 1998, ethnic Tamil guerrillas swamped Sri Lankan *embassies* with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems. *Id.*

appearing on affected computer screens before or even after the effects of the cyberattack take place.[267] The content of the messages cyberterrorists champion is myriad, i.e., aiming to replace the existing government by drawing out repressive responses, promoting the interests of a minority or religious group that has been persecuted by inflicting social harm, advancing a social or religious cause using violence to address their grievances, outlawing states possessing nuclear threats, or seeking to wipe out a minority group in a particular territory.[268]

To illustrate this proclaimed motive, about a decade ago, anti-nuclear hackers released a worm into the U.S. National Aeronautics and Space Administration's (NASA) SPAN network.[269] Antinuclear protestors were trying to stop the launch of the shuttle that carried the Galileo probe, whose booster system was fueled with radioactive plutonium, on its initial leg to Jupiter. When scientists logged into the computers at NASA's Goddard Space Flight Center in Maryland, they were greeted with a banner attached

267. CIWARS INTELLIGENCE REPORT (10 May 1998) [hereinafter CIWARS].

268. *Criminology*, *supra* note 263.

269. *Hearings before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, 106th Cong. (May 23, 2000) (testimony of Dorothy E. Denning) [hereinafter Testimony of Dorothy Denning].

to the worm sent by the hackers which read: Worms Against Nuclear Killers![270] This kind of expression reveals the motive behind the cyberattack.

ii.) If it is not proclaimed, the motive may be gathered from the actor and the act.

Absent any proclaimed motive, a terrorist act has been determined in the past by assessing the status of the party committing the act[271] – specifically the nature of the organization on whose behalf it is committed[272] – *and* the nature of the act itself.[273] Thus, twentieth century terrorist acts have always been evaluated based on the principle of propaganda by the deed.[274] This manner of determining the motive of the perpetrator should likewise apply in cyberterrorism.[275]

b.) The Actor's Membership in a Terrorist Organization

In the cyberage, the identity of the perpetrator is not always easy to discover.[276] However, changes in the technology that control cyberspace have, to a certain extent, effectively reduced the problem of anonymity.[277] For example, the implementation of Internet Protocol version or IPv6, and the F.B.I.'s Carnivore,[278] have improved the ability of law enforcement officials to track cyberspace communication through unique identifiers attached to every computer's IP number.[279] However, the author will not belabor this point as it is presumed that the evidence exists to ascertain the identity of the perpetrator (but not as to his motive) through any of the technological means available.

270. Denning, *Activism, Hacktivism, and Cyberterrorism*, *supra* note 152.

271. Shannon v. Fanning, I.R. 548, 597-8 (1984).

272. *In re* Doherty, 599 F. Supp. 270 (1984).

273. ASPECTS, *supra* note 127, at 133.

274. Green, Hijacking, *Extradition and Asylum*, 22 CHITTY'S L.J. 135, 140 (1974).

275. *See* Testimony of Dorothy Denning, *supra* note 270.

276. Du Pont, *The Criminalization of True Anonymity*, *supra* note 149, at 191,

277. *Clinton Taking Up Web Security with Experts, a Leading Hacker*, at 1, *available at* http://www.siliconvalley.com (last visited Dec. 30, 2000).

278. *Carnivore: Will It Devour Your Privacy?*, 2001 DUKE L. & TECH. REV. 28, 28 (2001).

279. *See* Note, *The Domain Name System: A Case Study of the Significance of Norms to Internet Governance*, 112 HARV. L. REV. 1657, 1657 n.2. (1999). *See also* Courtney Macavinta, *Internet Protocol Proposal Raises Privacy Concerns*, *available at* http://news.cnet.com/news/0-1005-200-852235.html (last visited Jan. 15, 2001) (on file with MTTLR).

Once the identity of the perpetrator is known, motive may be culled from his membership in any organization engaging in or espousing terrorist objectives.[280] Past terrorist acts have been adjudged as politically motivated based on their affiliation.[281] In the cyberage, certain terrorist groups have been developing a hacker network to support their computer activities to engage in offensive information warfare.[282] At present, States, like the U.S., Singapore, Malaysia, and the U.K., have pursued terrorists by using "guilt by association" as basis.[283] The presumption of motive from one's membership does not violate the right of the terrorist to due process and not be judged without trial as the presumption would still be rebuttable.

In reality, the perpetrator may even admit his membership in a terrorist organization such as what happened to Khalid Ibrahim. Ibrahim tried to buy military software from hackers who had stolen it from Department of Defense computers they had penetrated; when arrested, he claimed to be a member of the militant Indian separatist group Harkat-ul-Ansar, which declared war on the United States due to the latter's cruise-missile attack on a suspected terrorist training camp in Afghanistan.[284]

280. Professor Alan Sapp, *Motivations to Terrorism*, *available at* http://www.faculty.virginia.edu/ciag/terr_motiv.html (last visited Jul. 12, 2002) [hereinafter *Motivations to Terrorism*]. According to the Professor:

> The role of motive is important as a very useful investigative tool for leading us to the perpetrators of a given incident. I think of motive as being intermediary, if you will, to ideology on one side with ideology being a way of thinking that expresses values and beliefs. Ideology then leads to motives and the motive in turn when acted on leads to the behavior, and in an interaction between two people you can see the ideology and the behavior tied together very closely.
>
> The first I would label as the terrorists themselves. There are a number of different things to look at – is this state-sponsored? ... Is this an organized group like we've seen with some of the transnational groups that are appearing, or are we dealing with individuals or individuals that are perpetrating this particular act? In understanding that, the terrorist in their associations gives us some clue as to motives.

281. BRIAN L. DAVIS, QADDAFI, TERRORISM, AND THE ORIGINS OF THE U.S. ATTACK ON LIBYA 12 (1990).

282. Denning, *Activism, Hacktivism and Cyberterrorism*, *supra* note 152.

283. *See, e.g.*, Military Order of November 13, 2001: Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57, 833 (2001).

284. Denning, *Activism, Hacktivism and Cyberterrorism*, *supra* note 152.

Although it has been commonly argued that "one man's terrorist is another man's freedom fighter,"[285] a distinction must be made between terrorism and the legitimate struggle of peoples for national liberation.[286] A wall should separate groups indulging in terror from those with nationalist or self-determinist aims.[287] Under international law, the requirements which need to be satisfied before an organization may be afforded national liberation status[288] are its effective authority in liberated areas or organized allegiance of the people the organization claims to represent,[289] and the recognition by local, regional, and/or global governmental organization.[290] Thus, an organization with the support of only its members, and not those they wish to represent, cannot claim to be freedom fighters.

For instance, the U.S. State Department maintains a listing of active terrorist organizations.[291] All these groups exhibit the willingness to engage in indiscriminate violence or serious harm against civilians to achieve political ends.[292]

c) The act must have a particular target and effects.

The act, coupled with the actor, may provide the basis for determining whether the motive is political or not,[293] as the act itself may carry the message of the cyberterrorist.[294] In this respect, two elements in the act must

285. MURPHY, PUNISHING INTERNATIONAL TERRORISTS 4 (1985).

286 Bangkok Declaration, ¶ 21, *reprinted in* Human RIGHTS AND INTERNATIONAL RELATIONS IN THE ASIA-PACIFIC 204-7 (Tang ed., 1995).

287 LODGE, TERRORISM: A CHALLENGE TO THE STATE Ch. 6 (1981).

288 R. Ranjeva, *Peoples and National Liberation Movements, in* INTERNATIONAL LAW: ACHIEVEMENT AND PROSPECTS 107-112 (M. Bedjaoi ed., 1991).

289 Rapport dela mission specialedans les zone liberees de Guinee-Bissau en avril 1977, U.N.Doc. A/AC 109/400 (1977).

290 The Palestine Liberation Organization and National Liberation Movements in Africa, *Guidelines for Implementation of General Assembly Resolutions Granting Observer Status on a Regular Basis to Certain Regional Intergovernmental Organization*, U.N.J.Y.B. 165 (1975).

291 U.S. DEPARTMENT OF STATE, REPORT ON THE PATTERNS OF GLOBAL TERRORISM (1996).

292 *Hearings on the Anglo-U.S. Supplementary Extradition Treaty before the Senate*, S. Hrg.99-703 re TR.DOC.99-8, at 263 (1985) (prepared Statement of Sofaer, Legal Advisor of the U.S. Department of State).

293. *Motivations to Terrorism*, *supra* note 281.

294 *Id.*

> I think that it's important for us to recognize that every terrorist act carries a message – and it may carry a number of messages that are culturally defined. We may not recognize those kinds of things. As we were talking yesterday, Richard Landes turned to me and asked, "do you know what Dar es Salaam means" and I said no. It means "realm of peace." Is there a significance in selecting a target within the realm of peace for a terrorist attack? Is there a significance that the particular weapon includes the oxygen tanks that made the huge fireball with what from the crater we could see looked like a relatively much smaller explosive load? Is there a symbolism in the firebomb and is this simply a politically motivated anti-U.S. government attack on an embassy? Terrorists operate within a world view and our worldview sometimes doesn't even come close to understanding it, so when we think about an act as purely a political terrorism, we need to try to get into the world view of the individual perpetrators. Let me suggest to you purely as a thinking exercise some things about the world view of the people who carried those bombings out and the significance of those in terms of the message.

concur in order that the political motive may be deduced: its target and its effects.

i. Target

The target may indicate motive.[295] Cyberterrorists choose computer systems controlling critical infrastructure as targets. They do so because these systems are designed and established to enable the people to enjoy civilian freedoms,[296] hence, an attack against such infrastructure would produce wholesale disintegration of the working of civilian society.[297] More importantly, as the establishment and maintenance of critical infrastructure take up a big part of a State's budget,[298] States would have a keen interest in their protection. As a result, the targeting of critical infrastructure evinces a causal relationship between the motive of the cyberattacker and the attack itself, because it spawns the much-needed attention from and debilitating impact on the government[299] against which political dissent is being directed.

For instance, targeting transport navigation and safety control systems, imperiling lives of passengers or disrupting public utilities controlling basic

295. *Id.*

296. *See generally Hearing before the United States Senate Subcommittee on Technology, Terrorism, and Government Information Committee on the Judiciary*, 106th Cong. (Feb. 1, 2000) (statement of Frank J. Cilluffo, Deputy Director, Organized Crime Project Director, Task Force on Information Warfare & Information Assurance Center for Strategic & International Studies).

297. Thompson, *Internet Crime*, *supra* note 236, at 9.

298. Miyawaki, *supra* note 222.

299. Pollitt, *Fact or Fancy?*, *supra* note 33.

services, cause destructive failure and subsequent economic impact[300] which earns the ire of the public administrative body.[301]

ii. Effects

Together with the choice of target, the effects or extent of damage of the attack likewise gives an idea concerning the motive of the offender.[302] Serious attacks against critical infrastructure could be acts of cyberterrorism, depending on their impact.[303] To qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear from the public; consequently, getting the attention of those in authority.[304] Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples.[305] Attacks that disrupt nonessential services or that are mainly a costly nuisance would not evoke a political motive as they do not capture the interest of the government.[306] By proving that particular governed civilians are unsafe in a realm of peace, terrorists achieve publicity of the message to its government.

Therefore, when the political motive is not proclaimed, three things must concur so as to gather the political motive: (1) membership in a terrorist organization; (2) targeting of critical infrastructure; and (3) serious harm to a governed body, grabbing the attention of its established government.

d. Cyberterrorists are not mere political offenders.

Although political in character,[307] terrorist acts are not mere political offenses[308] that are non-extraditable.[309] One characteristic that distinguishes violent or injurious criminal acts from political offenses is provided for by the added requirement in the Swiss Test[310] that if the means used are excessive

300. Thompson, *Internet Crime*, *supra* note 236, at 4.

301. *Id.*

302. *Motivations to Terrorism*, *supra* note 281.

303. Testimony of Dorothy Denning, *supra* note 270.

304. Denning, *Is Cyber Terror Next?*, *supra* note 12.

305. COLLIN, THE FUTURE, *supra* note 259.

306. Denning, *Activism, Hacktivism, and Cyberterrorism*, *supra* note 152.

307. GEOFF, THE POLITICAL OFFENCE EXEMPTION 123 (1991).

308. European Convention on the Suppression of Terrorism, *supra* note 102.

309. *See* HARVARD RESEARCH: EXTRADITION 108-9 (1935); PRABASH SENHA, ASYLUM AND INTERNATIONAL LAW 74 (1971).

310. SWISS COMMITTEE ON IMMIGRATION AND NATIONALITY OF LAW, REPORT RECOMMENDING THE REFORM OF THE LAW OF INTERNATIONAL EXTRADITION (1986); Swiss Law On International Judicial Assistance in Criminal Matters, *reprinted in* 20 I.L.M. 1339 (1981).

to redress such political grievance,[311] such would not be a mere political offense, like terrorist crimes.[312] Under this test, political motive alone is not sufficient to categorize a crime as simply political;[313] only if the political element dominates, there being a direct connection between the crime and the political purpose,[314] would the offense be political. If the crime is violent, then the common element outweighs the political motive, unless such violence was the only means to achieve the end.[315]

The Swiss Test achieves the same end as that of three other tests to determine if an offense is political or not.[316] The United Kingdom Test[317] excludes from the political offense exemption crimes remotely related to the political objective.[318] Like these two tests, the French-Belgian Test[319] evaluates an offense on the basis of its impact on the character of the State, meaning whether civilians are directly affected by the attack.[320] These tests have been followed by the Irish Approach,[321] which does not regard offenses involving indiscriminate violence against civilians as mere political offenses,

311. I.A. SHEARER, EXTRADITION IN INTERNATIONAL LAW 182 (1971); *Compare In re* Peruzzo, *reprinted in* 19 INT'L L. REP. 369 (1951), *with In re* Kavic, *reprinted in* 19 INT'L L. REP. 371 (1952).

312. *In Re* Nappi, *reprinted in* 19 INT'L L. REP. 375, 376 (1952).

313. *See* Warbrick, *European Convention on Human Rights and the Prevention of Terrorism*, 32 INT'L & COMP. L. Q. 82 (1983).

314. *In re* Ockert, *reprinted in* [1933-4] ANN. DIG. 369 (No. 157); *In re* Nappi, 19 INT'L L.REP. at 143.

315. *In re* Pavan, *reprinted in* [1927-28] ANN. DIG. 347 at 349.

316. M. CHERIF BASSIOUNI, INTERNATIONAL EXTRADITION AND WORLD PUBLIC ORDER 383-41 (1974) [hereinafter BASSIOUNI, INTERNATIONAL EXTRADITION]. *See also* Lubet and Czackes, *The Role of the American Judiciary*, 71 J. CRIM. L. & CRIMINOLOGY 193, 201 (1980). *See generally* C. VAN DE WINJNGAERT, THE POLITICAL OFFENSE EXCEPTION TO EXTRADITION 1 (1980).

317. Watin v. Ministere Public Federal, *reprinted in* 72 INT'L L. REP. 614 (1964).

318. *See* MCF v. Public Prosecutor, *reprinted in* 100 INT'L L. REP. 414, 425 (1986).

319. Manuel Garcia-Mora, *The Nature of Political Offenses: A Knotty Problem of Extradition Law*, 48 VA. L. REV. 1235-36 (1962).

320. *In Re* Giovanni, *reprinted in* 14 ANN. DIG. 145 (Cours d'appel, Grenoble 1947).

321. Walker, *Constitutional Governance and Special Powers against Terrorism*, 37 COLUM. J. TRANSNAT'L L. 1, 1 (1997); Delaney and Hogan, *Anglo-Irish Extradition Viewed from an Irish Perspective*, *in* PUBLIC LAW 93 (1993); Campbell, *Extradition to Northern Ireland: Prospects and Problems*, 52 MOD. L. REV. 585, 585 (1989).

but terrorism.[322] Under all these tests, modern terrorist violence has been adjudged to be the antithesis of what could be merely political.[323]

As extensive State practice has shown,[324] the recent trend has been to eliminate the political offense exemption entirely because it offers defenses for international terrorism.[325] Attacks against civilians resulting in violence or harm[326] have been ruled as falling outside of the sphere of political crimes.[327] In fact, customary international law approves the exclusion of terrorist acts from the political offense exemption.[328] Simply put, a terrorist act is one injurious crime whose means exceed its political end; hence, not a political crime.[329]

In the cyberage, States have refused to recognize the application of the political offense exception to cybercriminals who, at the very least, incite hatred against a particular group.[330] More so, the political offense exception will not apply to politically motivated cyberattacks which destabilize the government and result in violence and intimidation.[331] In addition, cyberterrorist activities are not the most proximate and the only means to achieve a political end, as the same end can be achieved by mere hacktivism or political, non-harmful cyberactivities.[332] Clearly, although political in character, cyberterrorist acts are reprehensible crimes which, if

322. Ellis v. O'Dea (No. 2), I.L.R.M. 346, 362 (1991).

323. McGlinchey v. Wren, I.R. 154, 159 (1982).

324. BASSIOUNI, INTERNATIONAL EXTRADITION, *supra* note 317, at 370-71.

325. *Justice Ministers Hope to Drop Concept of Political Crime in Europe*, EUROPEAN SOCIAL POLICY, Apr. 14, 1994, *available in* LEXIS, News Library, Arcnews File.

326. Eains v. Wilkes, 641 F.2d 504, 521 (7th Circ. 1981), *cert. denied* 102 S. Ct. 390 (1981).

327. *In re* Extradition of Atta, 706 F. Supp. 1032, 1042-50 (1989).

328. M.E. Sapiro, *Extradition in an Era of Terrorism: The Need to Abolish the Political Offense Exception*, 61 N.Y.U. L. R. 654, 661 (1986). European Convention on the Suppression of Terrorism, *supra* note 102.

329. *See* Taulbee J. L., *Terrorism: The Right to Rebel and Political Asylum, in* TERRORISM AND POLITICAL VIOLENCE: LIMITS AND POSSIBILITIES OF LEGAL CONTROL 335, 339 (Han ed., 1993).

330. John T. Soma, et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. LEGIS. 317, 345 (1997) [hereinafter Soma, *Transnational Extradition*].

331. *Text of ADL Report: The Skinhead International: A Worldwide Survey of Neo-Nazi Skinheads*, U.S. NEWSWIRE, Jun. 18, 1995, at 4, *available at* LEXIS, News Library, Wires File.

332. *See* Amy Harmon, *Hacktivists of All Persuasions Take Their Struggle to the Web*, N.Y. TIMES, Oct. 31, 1999.

transnationally committed, will not permit the perpetrator to hide under the cloak of the political offense exception.

3. Third Element: The attack should create a state of terror in the minds of the general public or segment of a population.

Cyberterrorists seek attention, through the fear generated by a cyberattack;[333] fear is the instrument with which cyberterrorists work.[334] Unlike an ordinary hacker, cyberterrorists ensure that the population of a nation will be severely deprived of basic services, without giving warning to the people in charge of their protection.[335]

Cyberterrorism would include: the diversion of funds from bank computers causing panic among deposit holders[336] as banks need to shut down to address their problems; intrusion into confidential personal, medical, or financial information, as a tool of blackmail and extortion;[337] or theft of classified information from secure government databases to gain information vital to national security.[338]

Thus, the attacks against Florida's 911 system and the Worcester Airport would qualify as cyberterrorism, as long as the element of political motive is present. However, other activities, falling short of the definition of cyberterrorism, may either be activism or hacktivism.

E. Acts falling short of the definition of Cyberterrorism

In her testimony before a U.S. Congressional committee on cyberterrorism, Dorothy E. Denning, a leading international commentator on cyberterrorism, has suggested the classification of other cyberactivities whose definitions fall short of cyberterrorism.

333. *Hearings before the Joint Economic Committee on Cyber Threats and the U.S. Economy, Central Intelligence Agency* (Feb. 23, 2000).

334. *See* US SECOND ANNUAL REPORT OF THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION (2000).

335. Collin, Remarks, *supra* note 221.

336. *Id.*

337. THE NEXT WORLD WAR, *supra* note 7, at 156-8.

338. *See Rome Laboratory Attacks: Hearings before the Senate Governmental Affairs Committee Permanent Investigations Subcommittee* (May 22, 1996) (testimony of Jim Christy). *See also* TED UCHIDA, BUILDING A BASIS FOR INFORMATION WARFARE RULES OF ENGAGEMENT 8 (1997).

1. Activism: Unmotivated, Non-disruptive Cyberactivities

Activism refers to normal, unmotivated, non-disruptive use of the Internet in support of an agenda or cause, e.g., browsing the Web for information, constructing and posting materials on Websites, transmitting electronic publications through e-mail, and using the Net to discuss issues, form coalitions, and plan and coordinate activities.[339] Activists may be able to locate legislative documents, official policy statements, analyses and discussions about issues, and other items related to their mission. They may be able to find names and contact information for key decision makers inside the government or governments they ultimately hope to influence. They may be able to identify other groups and individuals with similar interests, and gather information for potential supporters and collaborators. There are numerous tools that help with collection, including search engines, e-mail distribution lists, and chat and discussion groups.

Activism includes the maintenance of a website with a political view, participation in political chat groups, or sending individuals e-mails with political content.[340] Thus, the mere posting of a site advocating terrorism without more, such as a site exalting Osama Bin Laden, falls under this definition.

2. Hactivism: Politically Motivated Cyberactivities Without Causing Harm

Hactivism is the active use of the Internet with hacking technologies to make a political statement or promote a political cause.[341] It is similar to cyberterrorism, absent the violent effects or hardship, such as the hijacking, defacement, or destruction of another's website for political motives, secretly tracking activity on government computers to inform the public, destruction of files or computers for political reasons, or sending of mass e-mail with political uses.[342] It appears, therefore, when tested under the Swiss Approach, the political element predominates, and the means do not exceed its political end.[343] Consequently, unlike cyberterrorism, hacktivism may qualify as a political offense. Simply put, hacktivism is the convergence of

339. Denning, *Activism, Hacktivism, and Cyberterrorism, supra* note 152.

340. A. Hesseldahl, *You've Got War*, WIRED NEWS, Aug. 24, 1998, *available at* www.wired.com/news/politics/story/14608.html (last visited Apr. 29, 2002).

341. N. Mckay, *The Golden Age of Hacktivism*, WIRED NEWS, Sept. 22, 1998, *available at* www.wired.com.news/politics/story/15129.html (last visited Apr. 30, 2002).

342. Bussutil, *A Taste of Armageddon, supra* note 133, at 41.

343. Kir v. Ministere Public Federal, *reprinted in* 34 INT'L L. REP. 143, 145 (1961).

hacking with activism, and ultimately is the bringing of methods of civil disobedience to cyberspace.[344]

An example would be the Portuguese hacking of the sites of 40 Indonesian servers in September 1998 to display the slogan "Free East Timor" in large black letters to protest Indonesian human rights abuses in the former Portuguese Colony;[345] or the Milworm hacking of more than 300 Web sites in July 1998 which altered the ISP's database so that users attempting to access the sites were redirected to a Milworm site, where they were greeted with a message protesting the nuclear arms race.[346]

Another instance of hacktivism was when ethnic Tamil guerrillas swamped Sri Lankan embassies with thousands of electronic mail messages.[347] The messages read: "We are the Internet Black Tigers and we're doing this to disrupt your communications."[348] An offshoot of the Liberation Tigers of Tamil Eelam, which had been fighting for an independent homeland for minority Tamils, was credited with the incident. The attack was said to have had the desired effect of promoting their political cause.[349]

Another example would be the Hong Kong Blondes' hacking of Chinese government computers in an effort to monitor China's intelligence activities and warn political targets of imminent arrests.[350] They attacked the systems of both Chinese state-owned organizations and Western companies investing in the country. In like manner, the attacks by the Bin Laden fanatics against U.S. e-mail systems after the September 11 bombing would likewise constitute hacktivism as no violence or serious damage to civilian persons and property resulted from their politically motivated sending of e-mail to support bin Laden.

While a cyberattack by civilians may constitute cyberterrorism, what happens if such cyberattack is attributable to a State and is directed against another State? If the State were the perpetrator, the incident would definitely be governed by international law controlling the relationships between

344. William Greider, *The Cyberscare of '99*, ROLLING STONE, Aug. 19, 1999, at 51.

345. Lindsay Murdoch, *A Computer Chaos Threat to Jakarta*, SYDNEY MORNING HERALD, Aug. 18, 1999, at 9.

346. Jim Hu, *Poiitical Hackers Hit 300 Sites, at* http://www.antionline.com. (last visited May 1, 2002).

347. Denning, *Activism, Hacktivism, and Cyberterrorism, supra* note 152.

348. *E-Mail Attack on Sri Lanka Computers*, 183 COMPUTER SECURITY ALERT, Jun. 8, 1998, at 8.

349. CIWARS, *supra* note 268.

350. Niall McKay, *China: The Great Firewall*, WIRED NEWS, Dec. 1, 1998. *See also* Sarah Elton, *Hacking in the Name of Democracy in China*, THE TORONTO STAR, Jul. 4, 1999.

States.[351] The attack may also go beyond civilians as the real target (hence, taking it out of the concept of cyberterrorism), and strike against military installations – the core of modern defense networks. Will the attacks be governed by the U.N. Charter on the prohibition against the use of force?

Is the response available to the attacked States unclear because of the ambiguity of the applicable international laws that apply to computer attacks?[352] Or are the rules clear enough to treat computer attacks as an "armed attack"?

How, then, does International Law treat such attacks?

III. CAN A STATE-SPONSORED CYBERTERRORIST ATTACK CONSTITUTE AN *'ARMED ATTACK'* TRIGGERING THE RIGHT OF SELF-DEFENSE?

The destructive nature[353] of cyberattacks presents new implications and analytical considerations of whether such attacks, when State-sponsored, fit into contemporary international legal rules pertaining to the prohibition against the use of force.[354] Conventional uses of force against information systems, such as the bombing of a computer center, can largely be dealt with using established law on the prohibition against the use of force.[355] It is the use of non-physical means of destruction that confronts many States,[356] as the threat of an information attack with serious implications is very real.[357] Interestingly, the U.N. appears to have already contemplated these types of electronic interference with a country's communications.[358]

351. *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) [hereinafter SHARP].

352. 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, 32 (2000).

353. Sean Kanuck, *Information Warfare:New Chalenges for Publis International Law*, 37 HARV. INT'L L.J. 272, 272 (1996).

354. George Seffers & Mark Walsh, *Does A Cyber Attack Constitute War?*, DEFENSE NEWS, Sept. 8 1999, at 1 [hereinafter Walsh, *Does A Cyber Attack Constitute War?*].

355. Aldrich, *War in the Information Age*, *supra* note 44, at 223.

356. Aldrich, *The International Legal Implications*, *supra* note 46, at 102.

357. THE NEXT WORLD WAR, *supra* note 7, at 14.

358. JOSEPH ROMM, DEFINING NATIONAL SECURITY 4 (1991) [hereinafter ROMM].

The Hague Conventions of 1899, a historical prelude to the drafting of the prohibition against the use of force under the U.N. Charter, which addressed means and methods of warfare, anticipated technological change – as evidenced by the "Martens Clause," which mandated the application of principles of international law even in cases not specifically covered by the agreement.[359] This provision was considered necessary to prevent future unnecessary and/or disproportionate destruction from weapons systems not yet developed.[360] Although the Martens Clause is originally a concept found in jus in bello (war), the same principle may likewise apply in jus ad bellum (use of force) since what the clause prohibits is unnecessary suffering caused to civilians, which may also result in jus ad bellum where the status quo ante would not even allow States to engage in the use of destructive weapons.

What made these cyberthreats against territorial integrity and political independence a pressing problem?

In large part, the vulnerability of a State to these attacks is due to technological development – its own and that of other States.[361] The U.S. military now operates 2.1 million computers and 10,000 local area networks (LANs).[362] These facts caused the authors of the Defense Science Board Report to observe, "We have built our economy and our military on a technology foundation that we do not control and, at least at the fine detail level, we do not understand."[363]

Recently, a computer worm called "Code Red" swept across the globe in two different devastating waves.[364] 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

359. 1899 Hague Convention for the Pacific Settlement of International Dispute, U.K.T.S. 9 (1901); 1907 Hague Convention for the Pacific Settlement of International Dispute, U.K.T.S. 6 (1971).

360. James Terry, *Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?*, 46 NAVAL L. REV. 170, 173 (1999) [hereinafter Terry, *Responding to Attacks*].

361. *See* Neil Munro, *Sketching a National Information Warfare Defense Plan*, 39 COMM. OF THE ACM 15, Nov. 1996, *available in* LEXIS, News Library, Magpap File. *See also* George Leopold, *Infowar: Can Bits Really Replace Bullets?*, ELEC. ENG'G. TIMES, Nov. 6, 1995, at 65.

362. *See Information Security*, *supra* note 10.

363. Thomas E. Ricks, *Information-Warfare Defense is Urged: Pentagon Panel Warns of 'Electronic Pearl Harbor,'* WALL ST. J., Jan. 6, 1997, at B2.

364. *See* Nicole C. Wong, *Code Red Creeping Worldwide*, WASH. POST, Aug. 2, 2001, at E1 [hereinafter Wong].

change its numerical Internet address as a precautionary measure.[365] A second wave spread a new variant of the worm a week later and infected over one hundred and fifty thousand computers.[366]

Recognizing the value of attacking adversary computer systems in order to counter other States' military superiority,[367] several States are pursuing government-sponsored offensive cyber-programs,[368] including Information Warfare in their military doctrine. Russia, China, France, Israel, and at least 33 other countries have been developing cyberarsenals to wage all-out cyberwarfare[369] through sophisticated electronic intrusion programs for intelligence collection.[370] Many of these governments pose a sophisticated electronic intrusion threat to national security and emergency preparedness, telecommunications, and information systems.[371]

365. *See Pentagon Web Sites Blocked; Threat of "Code Red" Computer "Worm" Prompts Safeguards*, WASH. POST, Jul. 24, 2001, at A5

366. *See* Wong, *supra* note 365.

367. *See* PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURE A-48, 9 (1997); The President's Commission on Critical Infrastructure Protection projects that, by the year 2002, 19 million individuals will have the knowledge with which to launch cyberattacks.

368. *See* Information Security: Computer Attacks at Department of Defense Pose Increasing Risks: Testimony Before the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 104th Cong. (1996) (statement of Jack L. Brock, Director, Defense Information and Financial Management Systems Accounting and Information, General Accounting Office) (more than 100 governments are capable of accessing, attacking, and conceivably disabling America's computers). *See also* Hai Lung and Chang Feng, Chinese Military Studies Information Warfare, PTS Msg 210225Z (1996); FitzGerald, *Russian Views on Electronic and Information Warfare*, *in* PROCEEDINGS OF THE THIRD INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM: PARTNERS FOR THE 21ST CENTURY 126 (1997) [hereinafter FitzGerald].

369. *National Security Threatened by Internet*, COMPUTER WORLD, Jan. 1, 2001, at 7.

370. National Intelligence Council, *The Foreign Information Warfare Threat to US Telecommunications and Information Systems: Hearings before the U.S. Joint Economic Committee* (Feb. 23, 2000) (testimony of Dan Kuehl, National Defense University) (depicting China and Russia as two nation-states that are cyber-threats to the US), *available at* http://www.odci.gov/cia/public_affairs/speeches/cyberthreats 022300.html. *See also* Madsen, *Intelligence Agency Threats to Computer Security*, 6 INT'L J. INTELLIGENCE & COUNTER INTELLIGENCE 446-87 (1993).

371. Hearings before the Joint Economic Committee on Cyber Threats and the US Economy (Feb. 23, 2000) (statement for the Record by John A. Serabian Jr, Information Operations Issue Manager, Central Intelligence Agency), *available at* http://www.odci.gov/cia/public_affairs/speeches/cyberthreatso22300.html (last visited Apr. 30, 2002).

On the level of preparation, nothing is unlawful regarding a State's research and development of technological, defensive military systems as such system intrusion could be viewed as lawful espionage or intelligence gathering which is not illegal per se under International Law.[372] But can States use these cybersystems offensively against another State without violating any rule of international law? Can they be used defensively?

A. The General Duty of Non-intervention

The United Nations unequivocally confirms the prohibition against intervention[373] by one State into the affairs of other States.[374] Pre-eminent among the relevant international instruments, the 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States[375] pertinently avers that:

> No state has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other state. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the state or against its political, economic and cultural elements, are condemned.

This prohibition was reaffirmed in Principle 3 of the 1970 Declaration on Principles in International Law,[376] with the proviso that not only were such interferences condemned, but they were held to be in breach of international legal rules.[377] Principle 3 holds:

> The principle the duty not to intervene in matters within the domestic jurisdiction of any State in accordance with the Charter

372. *See generally* SHARP, *supra* note 352, at 205-6.

373. Report of the UN Special Committee on the Problem of Hungary, G.A.O.R., 11th Sess., Supp. 18 (1957).

374. OPPENHEIM, *supra* note 119, at 59; Breshnev Doctrine, Text of the Speech of Polish representative Mr. Breshnev, 20 CURRENT DIG. SOVIET PRESS 3-4 (1968).

375. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131, U.N. GAOR, 20th Sess., Supp. No. 14, at 12, UN Doc.A/6220 (1965).

376. Friendly Relations, *supra* note 84.

377. Corfu Channel Case (Albania v. U.K.), 1949 I.C.J. 4, at 35 ("[t]he alleged right of intervention [was] the manifestation of a policy of force, such as has, in the past, given rise to serious abuses and as such cannot ... find a place in international law.").

> No State, or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference, or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.
>
> No State may use or encourage the use of economic, political, or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure advantages of any kind...
>
> x x x
>
> Every State has an inalienable right to choose its political, economic, social, and cultural systems, without interference in any form by another State.[378]

Intervention is prohibited when it interferes in matters in which each State is permitted to decide freely by virtue of the principle of state sovereignty.[379] Respect for the principle of the sovereignty of States closely allies with legal rules that prohibit the use of force and interstate intervention.[380] Thus, States are obliged to refrain from any interference in any form in the internal affairs of any country.[381] It must be noted that the principle of non-intervention is broader than the prohibition contained in Article 2(4) of the U.N. Charter.[382] The declaration prohibits measures falling short of armed force such as economic sanctions.[383] Therefore, should the prohibition on cyberattacks simply fall under this duty?

No doubt, these activities clearly intrude into the internal affairs of another State; hence clearly a violation of the duty of non-intervention. More than constituting intervention, should cyberattacks constitute Use of Force under the U.N. Charter? Some authors would say that cyberattacks do not exceed any threshold of harm against which customary international law protects civilians as cybermeans do not visibly manifest themselves to put the attacked State on notice.[384] However, it is the author's submission that

378. G.A. Res. 2625 (XXV), GAOR, 25th Sess., Supp. No. 28, Principle 3, U.N. Doc.A/8082 (1970).

379. G.A. Res. 2908, GAOR, 27th Sess., Supp. No. 30, at 2 (1972). HARRIS, CASES AND MATERIALS, *supra* note 1, at 886.

380. *Id.*

381. G.A. Res. ES-6/2, G.A.O.R., 6th Emerg. Sp. Sess., Supp. 1, at 2 (1980); G.A. Res. 38/7, G.A.O.R., 38th Sess. Supp. 47 47, at 19 (1983). *See* THOMAS AND THOMAS, THE DOMINICAN REPUBLIC CRISIS 1965 (1967).

382. HARRIS, CASES AND MATERIALS, *supra* note 1, at 890.

383. Declaration of the United Kingdom, 1967 Special Committee on Principles of International Law, U.N. Doc. A/AC.125/SR.73, *reprinted in* B.P.I.L. 39 (1967).

384. *Information Warfare as International Coercion, supra* note 5.

cyberattacks against critical infrastructure are governed by the prohibition against the Use of Force.

The proliferation of cyberattacks against information systems controlling critical infrastructure, particularly transportation systems, [385] telecommunications, [386] and electronic power industries, [387] upon which sovereign functions greatly depend,[388] necessitates resort to the U.N. Charter to adjudge the illegality of such cyberattacks.[389] Article 2(4) would still prohibit a State's act of "messing with" the computer systems of another State's banks to disrupt and destroy the economy[390] as such an attack is not a mere diplomatic, economic sanction,[391] but a direct attack against a State's territorial integrity;[392] hence, a violation of Article 2(4) of the Charter.

Why is this so? The history and policy behind Article 2(4) clearly provide the explanation.

B. The Prohibition Against the Use of Force

Article 2(4) of the U.N. Charter provides that all 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. [393] As Professor Louis Henkin has written, this is the most important norm of international law, the distillation and embodiment of the primary value of the inter-State system, the defense of State independence and state

385. Bowman, *Essay: International Security in the Post-Cold War Era: Can International Law Truly Effect Global Political and Economic Stability? Is International Law Ready for the Information Age?*, 16 FORDHAM INT'L L.J. 1935, 1939 (1996) [hereinafter Bowman, *International Security*]. *See Pittsburgh Airport's Radar Screens Go Out for 6 Minutes*, CHARLESTON GAZETTE, Feb. 1, 1996, at 6A.

386. Ernest Krutzsch, *Cyber Warfare*, Dec. 13, 2000, *available at* http://rr.sans.org/infowar/cyber_war.php (last visited Apr. 15, 2002).

387. *See* FitzGerald, *supra* note 369, at 126.

388. Lyman, *Civil Remedies, supra* note 23, at 607.

389. TRUST IN CYBERSPACE 18 (Schneider ed., 1999) [hereinafter TRUST]. *See* Walker, *Information Warfare, supra* note 2, at 1182.

390. Jim Mackey, Address before the International Association for Counterterrorism and Security Professional Briefing (Oct. 8, 1999).

391. WALLACE, *supra* note 205, at 251; *Nicaragua*, 1986 I.C.J. at 14.

392. Mark Jacobson, *War in the Information Age: International Law, Self-Defense and the Problem of Non-armed Attacks*, (unpublished manuscript on file with the Merschon Center, Ohio State University) [hereinafter Jacobson, *War in the Information Age*].

393. U.N. CHARTER, art. 2, ¶ 4.

autonomy.[394] The provision is generally accepted[395] as expressing not merely the obligations of Members of the United Nations, but a non-derogable customary rule[396] of international law concerning the use of force.[397]

The underlying purpose of Article 2(4) is to regulate aggressive behavior between States, which is identical to that of its precursor in the Covenant of the League of Nations. Article 12 of the Covenant stated that League members were obliged not to "resort to war."[398] The League's terminology left unmentioned actions that, although clearly hostile, could not be considered to constitute acts of war. Subsequently, in drafting the U.N. Charter, the term "war" was replaced by the phrase "threat or use of force." The wording was interpreted as prohibiting a broad range of hostile activities including not only "war" and other equally destructive conflicts, but also applications of force of a lesser intensity or magnitude.[399]

Consequently, although the historical value of this provision was to restrict the use of force to acts of war,[400] there is now a consensus among highly qualified publicists that Article 2(4) outlaws aggressive behavior falling short of war, for instance, reprisals.[401]

But what does force mean?

394. LOUIS HENKIN, INTERNATIONAL LAW: POLITICS, VALUES AND FUNCTIONS 146 (1990).

395. *Corfu*, 1949 I.C.J. 4. *See* The Entebbe Incident, U.N. Doc.S/PV.1939, *reprinted in* 15 I.L.M. 1224 (1976).

396. Theodor Meron, *The Meaning and Reach of the International Convention on the Elimination of All Forms of Racial Discrimination*, 79 AM. J. INT'L L. 283, 283 (1985) (emphasizing that it is generally accepted that the principles of the United Nations Charter prohibiting the use of force have the character of *jus cogens*). *See* RESTATEMENT (THIRD), § 102 (expounding on the concept of *jus cogens* as peremptory norms of international law); HARRIS, CASES AND MATERIALS, *supra* note 1, at 862; *Nicaragua*, 1986 I.C.J. at 14.

397. Carin Kahgan, Jus Cogens *and the Inherent Right to Self-defense*, 3 ILSA J. INT'L & COM. L. 767, 767 (1997).

398. *See* Covenant of the League of Nations, art. 12, U.K.T.S. 4 (1919).

399. MYRES MCDOUGAL & FLORENTINO FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER 142-143 (1961) [hereinafter MCDOUGAL & FELICIANO].

400. Rosalyn Higgins, *Grotius and the Development of International Law in The United Nations Period*, *in* HUGO GROTIUS AND INTERNATIONAL RELATIONS 267 (H. Bull, et al., ed., 1990). *See* General Treaty for the Renunciation of War, U.K.T.S. 29 (1929)

401. WALLACE, *supra* note 205, at 249; HIGGINS, PROBLEMS AND PROCESSES, *supra* note 200, at 240. *See* Bowett, *Reprisals Involving Recourse to Armed Force*, 66 AM. J. INT'L L. 1 (1972) [hereinafter Bowett, *Reprisals*].

Traditionally, this has been interpreted to prohibit the use of armed force or gunboat diplomacy.[402] However, the "threat or use of force" must be interpreted to mean both armed and non-armed force,[403] as the term "threat or use of force" does not always constitute, and must be distinguished from, an armed attack.[404] What it only, and clearly, excludes is mere political or economic pressure through economic sanctions which fall under the general duty of non-intervention.[405]

Scholars have been unanimous in stating that the prohibition against the use of force embraces all threats of acts of violence without distinction.[406] Article 2(4) of the Charter covers any and all uses of force or threats to use force against the territorial integrity or political independence of States – not only by means of visible armed attacks across State frontiers – but inconceivable attacks short of actual armed attacks, such as the 1962 Cuban secret deployment of missiles.[407] The intention of the authors of said provision was to state in the broadest terms an absolute all-inclusive prohibition;[408] the phrase "in any other manner" was designed to ensure that there would be no loopholes.[409] Article 2(4) stipulates a clear prohibition against a State's right to use force, which evidently would include cyberforce.[410] In addition, the prohibition against 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

402. LELAND M. GOODRICH ET AL., CHARTER OF THE UNITED NATIONS: COMMENTARY AND DOCUMENTS 44 (3d. 1969) [hereinafter GOODRICH].

403. Kelsen, *General International Law and the Law of the United Nations*, *in* THE UNITED NATIONS: TEN YEARS LEGAL PROCESS 4-5 (Gesina H.J. Van Der Molen et al. eds., 1956). *See* Ahmed M. Rifaat, INTERNATIONAL AGGRESSION: A STUDY OF THE LEGAL CONCEPT, ITS DEVELOPMENT AND DEFINITION IN INTERNATIONAL LAW 234 (1979).

404. See *Nicaragua*, 186 I.C.J., at 93-99.

405. CHARTER OF THE UNITED NATIONS 49 (3d. 1969).

406. Jordan Paust, *Comment*, *in* A.S.I.L. PROCEEDINGS: 78TH ANNUAL MEETING 92 (1984); WALLACE, *supra* note 205, at 249.

407. *See* Eugene Rostow, *The Legality of the International Use of Force*, 10 YALE J. INT'L L. 286, 287. *See also* ISAGANI CRUZ, PUBLIC INTERNATIONAL LAW 94 (1985).

408. Edward Gordon, *Article 2(4) in Historical Context*, 10 YALE J. INT'L L. 271, 276 (1985).

409. Ian Brownlie, *The Use of Force in Self-Defense*, 37 BRIT. Y.B. INT'L L. 183, 236 (1961).

410. *Information Warfare as International Coercion*, *supra* note 5.

conventional military force.[411] Therefore, a cyberattack, 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.[412]

Article 2(4) has been given precise meaning by Principle 1 of the Declaration on Friendly Relations.[413] While Principle 3 of the Declaration deals with the duty of non-intervention,[414] the principle enunciated in Principle 1 directly refers, and echoes, Article 2(4) of the Charter and even enumerates in a non-exhaustive list acts constituting threat or use of force:

> The General Assembly...
>
> Solemnly proclaims the following principles:
>
> The principle that States 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
>
> Every State has the duty to refrain in its 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. Such a threat or use of force constitutes a violation of international law and the Charter of the United Nations and shall never be employed as a means of settling international issues.
>
> x x x
>
> Every State has the duty to refrain from organizing, instigating, assisting, or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.

Thus, a State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts or acquiescing in organized activities when the acts involve a *threat or use of force*.[415] Resolution 2625, the Declaration on Friendly Relations, describes behavior that constitutes the "unlawful threat or use of force" and enumerates standards of

411. *See* SHARP, *supra* note 352, at 101 ("[T]he use of force prohibition covers physical force of a non-military nature committed by any State agency.") (quoting SIMMA, *supra* note 94, at 113).

412. *See id.* at 101-2.

413. HARRIS, CASES AND MATERIALS, *supra* note 1, at 863.

414. G.A. Res. 2625 (XXV), GAOR, 25th Sess., Supp. No. 28, Principle 2, U.N. Doc.A/8082 (1970).

415. *Id.* Principle 3. *See* Resolution on the Definition of Aggression, G.A. Res. 3314 (XXIX), GAOR, 29th Sess., Supp. 31, at 142, *reprinted in* 69 AM. J. INT'L L. 480 (1975).

conduct by which States must abide. Contravention of *Principle 1* is declared to be a violation of Article 2(4).[416]

> *Article 1 of G.A. Resolution 3314 defines aggression as the use of armed force by a State against the sovereignty, territorial integrity, or political independence of another State, or in any manner inconsistent with the Charter of the United Nations. Article 3 lists what would qualify an as act of aggression, which includes:*
>
> x x x
>
> b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;[417]

A weapon is simply a tool designed to accomplish a specified task, or anything used, in destroying, defeating, threatening or injuring a person.[418] Thus, information attacks do constitute aggression as espoused by treaty and customary international law.[419] The actions of States or their surrogates in supporting or taking part in acts of aggression through information technology which threaten vital national interests of a State or States, whether through disruption of military information downlinks in satellites, sabotage of vital computer networks, or infiltration of electronic commercial transmission systems, clearly fall within the scope of Article 2(4).[420]

The author asserts that a cyberattack against critical infrastructures violates Article 2(4) based on two reasons.

1. Cyber attacks against critical infrastructure destabilize the political independence or territorial integrity of a State.

The protection of territorial integrity and political independence have been considered cornerstones of national security, which includes the capacity to control both domestic and foreign conditions necessary to enjoy a State's self-determination, autonomy, prosperity, and well-being.[421] Firmly fixed in customary international law,[422] this general principle of exclusive

416. Terry, *Responding to Attacks, supra* note 361, at 173; Robert Rosenstock, *The Declaration of Principles of International Law Concerning Friendly Nations: A Survey*, 65 AM. J. INT'L L. 713, 715 (1971).

417. G.A. Res. 3314 (XXIX), GAOR, 29th Sess., Supp. 31, at 142, *reprinted in* 69 AM. J. INT'L L. 480 (1975) (emphasis supplied).

418. Jacobson, *War in the Information Age, supra* note 393.

419. *Id.*

420. Terry, *Responding to Attacks, supra* note 361, at 174.

421. ROMM, *supra* note 359, at 4.

422. *See* RESTATEMENT (THIRD), § 102. *See also Nicaragua*, 1986 I.C.J., at 93-99, ¶ 202. *Accord* Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty,

sovereignty over national territory implies that each State is autonomous, free from coercion, and able to preserve the corporate integrity of its territory to the exclusion of all other States, and any limitation of this authority is subject to the consent of the territorial State.[423]

Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each State retains exclusive authority over activities within its borders.[424] Under this principle, so long as physical boundaries of jurisdiction exist and objects and activities can be precisely located, the legal concepts of possession, sovereignty, and inviolability make sense.[425] The meaning of these terms appears plain and simple: 'Territorial' means limited to a specific territory. 'Integrity' means an unimpaired or unmarred condition, original perfect state, entireness, completeness, undivided or unbroken.[426] However, the new technological capability of governments to employ cyberinstruments across international networks challenges the viability of the traditional view on territorial sovereignty as a legal construct.[427]

As physical threats to critical infrastructure are considered national security threats,[428] cyberattacks against a State's critical infrastructure results in the similar impairment of the territory of a State by clandestinely, without physical encroachment,[429] intruding into and disabling an entire national computer system.[430] Tested by State practice, the parameters of the prohibition against the Use of Force suggest wider latitude in meaning and scope in a world that is electronically interconnected with billions of signals traveling between national networks, and electromagnetic waves crossing

General Assembly Resolution 2131, U.N. GAOR, 20th Sess., Supp. No. 14, at 12, U.N. Doc. A/6220 (1965) 26; Friendly Relations, *supra* note 84; ANTHONY CLARK AREND, LEGAL RULES AND INTERNATIONAL SOCIETY 47-8 (1999).

423. *Information Warfare as International Coercion, supra* note 5.

424. *Id.*

425. *Id.*

426. II WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1174-1148 (1966).

427. Kanuck, Recent Development, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 275-6 (1996).

428. M. E. Bowman, *The Military Role in Meeting the Threat of Domestic Terrorism*, 39 NAVAL L. REV. 209 (1990).

429. LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW: INTRODUCTION 27 (1998) [hereinafter GREENBERG].

430. *See generally* Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641, 647 (2002) [hereinafter Creekman, *Response to China*].

national borders instantaneously, thereby creating conditions that allow individuals or groups in one place to affect systems transglobally.[431]

Clearly, the concept of sovereignty vis a vis territoriality is no longer static.

Although "use of force" against the territorial integrity of another State has often been interpreted in the traditional sense as taking of land,[432] a cyberattack nevertheless violates territorial integrity as Governments may fall due to a cyberattack against a nation's critical infrastructure, depriving a State of its capacity to maintain its territorial integrity.[433] Chaos and panic ensue, and could cascade even into dramatic repercussions affecting the stability of any State.[434]

2. The disruption of computer systems vital to the stability and survival of a State is inconsistent with the purposes of the United Nations.

All members of the United Nations are obliged to settle international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.[435] The United Nations was founded "to save succeeding generations from the scourge of war" and "to suppress acts of aggression or other breaches of the peace."[436] This fundamental proscription against the use of interstate force prohibits the possible resort to a violent weapon that inflicts human injury.[437]

Modern technologies defy attempts to set out as exhaustive a list of which weapons may or may not fall within the legal meaning of U.N. Charter law. There are significant examples of non-physical uses of force that seem to be encompassed by Article 2(4). Specifically, the provision of logistical support,[438] the use or threatened use of chemical weapons and biological weapons,[439] and aircraft radar lock-on, would all appear to violate

431. *Information Warfare as International Coercion, supra* note 5.

432. *See* GOODRICH, *supra* note 403, at 47-8.

433. Kurt C. Reitinger, *New Tools for New Jobs*, 124 PROC. U.S. NAVAL INST. 37, 37 (1998); Seffers & Walsh, *Does a Cyber Attack Constitute War, supra* note 355, at 1.

434. *Information Warfare as International Coercion, supra* note 5.

435. U.N. CHARTER, art. 2(3).

436. *Id.* Preamble. *See* Schachter, *International Law: The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620 (1984).

437. D.W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 148 (1958) [hereinafter BOWETT, SELF-DEFENCE]; IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 361 (1963) [hereinafter INTERNATIONAL LAW AND THE USE OF FORCE].

438. Aldrich, *War in the Information Age, supra* note 44, at 239.

439. *See* BROWNLIE, INTERNATIONAL LAW, *supra* note 186, at 362.

Article 2(4).[440] Without a doubt, an international consensus admits that such a prohibition against the use force extends to both conventional and non-conventional weapons such as bacteriological, biological, and chemical devices and nuclear and thermonuclear weapons.[441] In fact, even radar lock-on during an aerial dogfight has been classified in certain circumstances as unlawful use of force.[442] The situation involves no physical force, but rather sensors which can interpret certain types of directed energy and alert the pilot through a computer display.[443]

These non-conventional weapons are considered as forms of force since such weapons can destroy life and property.[444] Similarly, cyber-instigated downing of critical infrastructure[445] could destroy lives and damage property as devastating as those caused by other non-conventional weapons.[446] It is the attacks against information systems controlling critical infrastructure of States,[447] necessary for its survival,[448] which amounts to an illegal use of force.[449]

To summarize, may a cyber attack fall under Article 2(4) of the UN Charter?

Yes, if the cyberattack is against the political independence or territorial integrity of a State, i.e. critical infrastructure. As the prohibition against the use of force embraces all threats or acts of violence without distinction,[450] it

440. *See* Michael N. Schmitt, *Clipped Wings: Effective and Legal No-Fly Zone Rules of Engagement*, 20 LOY. L.A. INT'L & COMP. L.J. 727, 756-57 (1998).

441. *Information Warfare as International Coercion*, *supra* note 5.

442. *See* Mark S. Martins, *Rules of Engagement for Land Forces: A Matter of Training, Not Lawyering*, 143 MIL. L. REV. 1, 42 (1994).

443. Martin Fletcher, *Pentagon Admits Iraqi Radar Did Not Lock On to U.S. Plane*, TIMES (LONDON), Nov. 4, 1996, at 12.

444. BROWNLIE, INTERNATIONAL LAW, *supra* note 186, at 362.

445. *See generally* Constantini, *Information Warriors Form New Army, International Press Service*, Aug. 8, 1996, *available in* 1996 WL 10768646.

446. Laqueur, *supra* note 28, at 14.

447. Bowman, *International Security*, *supra* note 386, at 1939. *See Pittsburgh Airport's Radar Screens Go Out for 6 Minutes*, CHARLESTON GAZETTE, Feb. 1, 1996, at 6A; Ernest Krutzsch, *Cyber Warfare*, *available at* http://rr.sans.org/infowar/cyber_war.php (last visited Apr. 15, 2002); M.W. Wik, *Global Information Infrastructure Threats*, *available at* http://www.Globalcommons.co.uk./interactive technology/firewall/280_2.html (last visited May 30, 2002).

448. Lyman, *Civil Remedies*, *supra* note 23, at 607.

449. *See* Walker, *Information Warfare*, *supra* note 2, at 1182; TRUST, *supra* note 390, at 18.

450. WALLACE, *supra* note 205, at 249.

proscribes cyberattacks against critical infrastructure in the same vein, as they provide a more effective means of offsetting a State's strengths by striking this nation where it is most vulnerable.[451]

This is, therefore, not problematic.

What is problematic, however, is the appropriate response to a cyberattack.

Could the victim-State of such cyber-use of force respond, in self-defense, with traditional use of force? Or should it be confined to responding only through the same amount of cyber-use of force? Or could the victim-State respond in self-defense at all, considering that a State may only act in self-defense in the presence of an armed attack?

Is there a right to Self-Defense against a cyberattack?

C. Self-Defense in the Presence of an Armed Attack

Under international law, States may only exercise the right of self-defense[452] when responding to an actual armed attack. [453] According to the International Law Commission's Draft Articles on State Responsibility, the wrongfulness of an act of a State is precluded if the act constitutes a lawful measure of self-defense taken in conformity with the Charter of the United Nations.[454] Article 51 of the U.N. Charter, in pertinent part, 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

451. Frank J. Cilluffo et al., *Bad Guys and Good Stuff: When and Where Will the Cyber Threats Converge?*, 12 DEPAUL BUS. L.J. 131, 144 (2000); Buchan, *Implications of Information Vulnerabilities for Military Operations*, *in* STRATEGIC APPRAISAL: THE CHANGING ROLE OF INFORMATION IN WARFARE 283, 315 (Khalilzad & White eds., 1999).

452. U.N. CHARTER, art. 51. *See* A. CASSESE, INTERNATIONAL LAW IN A DIVIDED WORLD 230 (1986) [hereinafter CASSESE]; I de Arechaga, *International Law in the Past Third of the Century*, 159 H.R. 1, 87-98 (1979).

453. Brownlie, *The Use of Force by States*, *in* THE RULE OF LAW IN INTERNATIONAL AFFAIRS AFTER THE 50TH ANNIVERSARY OF THE U. N. 203 (1998); KELSEN, THE LAW OF THE UNITED NATIONS 914 (1950). *See* INTERNATIONAL LAW AND THE USE OF FORCE, *supra* note 438, at 214-239; SIMMA, *supra* note 94, at 51.

454. Draft Articles on the Responsibility of States for Internationally Wrongful Acts, arts. 4-11, adopted by the ILC at its 53rd Session (2001), Report of the I.L.C. on the Work of its 53rd Session, U.N. GAOR, 56th Sess., Supp. No. 10 (A/56/10), art. 21 (2001), *also available at* http://www.un.org/law/ilc/texts/state_responsibilty/responsibility_articles(e).pdf [hereinafter Draft Articles].

> United Nations, until the Security Council has taken measures necessary to maintain international peace and security.[455]

This limitation upholds world community standards contributing to a more stable international order, as what one author has suggested:

> First, the restriction tends to dissuade the scenario of the vicious cycle of escalating violence from occurring. Secondly, it ensures that force is used only as an emergency measure – as a necessary last resort. Thirdly, it functions as a restraint against uses of force that are based on pretext, misunderstanding and erroneous factual determinations. Professor Louis Henkin put it well when he observed that the United Nations 'recognize[s] the exception of self-defense in emergency, but limit[s] [it] to actual armed attack, which is clear, unambiguous, subject to proof, and not easily open to misinterpretation or fabrication.' In the post-Second World War era of conventional military weapons and international war, such considerations were particularly apt.[456]

In the Nicaragua Case,[457] the ICJ had the opportunity to clarify the extent and scope of an armed attack:

> There now appears to be a general agreement on the nature of the acts which can be treated as constituting armed attacks. In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular forces across an international border, but also the sending by or on behalf of a State of *armed* bands, groups, irregulars or mercenaries, which carry out *armed force* against another State of such gravity as to *amount to an actual armed attack* conducted by regular forces, or its substantial involvement therein.
>
> The Court sees no reason to deny, that in customary law, the prohibition of armed attacks *apply* to the sending by a State of *armed* bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.
>
> But the Court *does not believe that the concept of armed attack includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of provision of weapons or logistical or other support.* Such assistance may be regarded as threat or use of force, or amount to intervention in the internal or external affairs of other States.

It appears that it is the actual sending of military force, whether through regular or irregular bands, into the territory of the attacked State that triggers the right under Article 51.[458] In Nicaragua, only article 3(g) of G.A.

455. U.N. CHARTER, art. 51.

456. *Information Warfare as International Coercion, supra* note 5.

457. *Nicargua*, 1986 I.C.J. at 103 (emphasis supplied).

458. PHILIP JESSUP, MODERN LAW OF NATIONS 164-7 (1948).

Resolution 3314[459] was categorically recognized by the Court as a rule of customary law defining an armed attack, and not the entire listing as provided for in G.A. Resolution 3314.[460] Accordingly, by logical deduction, other actions falling short of article 3(g) do not constitute an armed attack that would enable a State to act in self-defense.[461]

At present, then, States do not perforce have the right of armed response to acts that fall short of constituting an armed attack.[462] A cursory reading of Nicaragua would seem that only military attacks, and not every isolated armed incident, rise to the level of an armed attack.[463] Certain acts of intrusion may be unlawful, but these acts do not necessarily endow a State the right to respond by using force in self-defense. Consequently, some illegal actions taken by a government against another State rise to the level of violating the prohibition against the use of force, but not every act of intervention rises to the level of an 'armed attack' that necessarily triggers a State's right to respond in self-defense.

To illustrate the traditional view, a response to a cyberattack, such as the release of a similar virus to counter an initial cyberattack, could be viewed as a retaliatory or punitive use of force.[464] Such an attack would give the impression that it is prohibited by international law because it would not be in response to the equivalent of an armed attack.[465] Therefore, under the status quo, a cyberattack does not seem to meet the conventional definition of an armed attack[466] triggering the right to self-defense.

What has been suggested is that the attacked State is not without recourse as the Security Council retains the authority to authorize the use of force to respond to any threat to the peace, breach of the peace, or act of

459. Article 3(g) encapsulates the only customary rule on the definition of the word 'armed attack' in the long list under the Declaration: "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another state of such gravity as to amount to an actual armed attack conducted by regular forces or its substantial involvement therein."

460. *Nicaragua*, 1986 I.C.J. at 103.

461. *See id.*

462. *Id.*

463. *Id.*

464. SHARP, *supra* note 352, at 37-9.

465. Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641, 664 (2002).

466. *See generally* Walker, *Information Warfare, supra* note 2, at 1177-78.

aggression.[467] The attacked State may appeal to the U.N. Security Council, which is authorized under Article 39 of its Charter, to respond with force to any event that threatens peace, even if the event does not meet the threshold of an armed attack.[468] If early detection and other preventive measures[469] fail, the State may be able to ask for reparations for any damage done as well as publicly disclose the aggressor State's role in the computer attack to cause international embarrassment.[470] Some writers even opine that the legality of any action the attacked State might take would be questionable because there are no international agreements which deal explicitly and specifically with this type of computer attack.[471]

The author submits, however, that a cyberattack against a critical infrastructure should trigger the right to self-defense, albeit in a limited sense. Article 39 will not be sufficient as no State is obliged to ignore an attack as irrelevant, and the imminent threat to the national security requires consideration of a response.[472] This, the author will analyze and justify in the next Chapter.

V. ANALYZING AND JUSTIFYING THE EXERCISE OF THE RIGHT OF SELF-DEFENSE AGAINST A CYBERATTACK

A. Defining A Cyberattack as an Armed Attack Based on the Means/Method

The traditional view of what constitutes an armed attack emphasizes the word "armed." However, "armed" does not necessarily mean those attacks that involve a high-explosive bomb, an aircraft, or a machine gun, that is, those physical means of destruction.[473] Indeed as technology changes, there is a need to reconsider what constitutes an instrument of war.[474]

467. *See* Schmitt, *supra* note 168, at 920 (construing a non-armed attack to which a responsive use of force is justified, and does not leave the international community remediless). Perforce, 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. *Id.* at 929.

468. U.N. CHARTER, arts. 39 & 42.

469. *See* SHARP, *supra* note 352, at 130.

470. *Id.* at 130

471. *See* Bowman, *International Security*, *supra* note 386, at 1939.

472. Terry, *Responding to Attacks*, *supra* note 361, at 177.

473. Jacobson, *War in the Information Age*, *supra* note 293.

474. For a more thorough discussion, *see* STEVEN ROSEN, WINNING THE NEXT WAR: INNOVATION AND THE MODERN MILITARY (1991).

"Armed," after all, need not refer only to conventional weapons as aggression may be achieved without the use of physical means of destruction.[475] For aggressive behavior to constitute war, it does not require that force manifest itself physically.[476] Armed simply means equipped with weapons of war, considering that a State equips itself for war depending on its enemy, objectives, vulnerabilities and weaknesses.[477] Otherwise, the use of non-conventional methods resulting in destruction without physically alerting the attacked State, at the first instance, would go unpunished.

The traditional view as to what constitutes an armed attack should not apply to cyberattacks because attacks on computer systems are, by nature, covert in execution, and practiced with silent effectiveness.[478] As a policy tool, computer attacks on vital national infrastructure targets might be as effective, if not more effective, than conventional/physical attacks.[479] In fact, many predict the next international conflict between two technologically advanced countries will involve computer attacks.[480] Hence, it cannot be gainsaid that armed attacks may be those which involve the use of any sort of equipment which enables an aggressor to gain military (tactical) advantage over another State[481] in those cases where the States are not yet engaged in war.

In truth, history reveals that nations have not always relied on physical means of destruction.[482] Notably, at the beginning of the First World War, the Royal Navy cut all the submarine telegraph cables that linked Germany to the rest of the world, preventing any communications between Germany

475. For an extensive analysis of what "armed" means, *see* PHILIP M. TAYLOR, MUNITIONS OF THE MIND (1990).

476. CARL VON CLAUSEWITZ, ON WAR 75 (Michael Howard & Peter Paet eds., 1976)

477. Jacobson, *War in the Information Age*, *supra* note 293.

478. Terry, *Responding to Attacks*, *supra* note 361, at 178.

479. *See* Andrea Stone, *Cyberspace is the Next Battlefield: U.S., Foreign Forces Prepare for Conflict Unlike Any Before*, USA TODAY, Jun. 19, 2001, at 1A [hereinafter Stone].

480. *See id.* at 2A.

481. Bruce Berkowitz, *Warfare in the Information Age*, ISSUES SCI. & TECH. 59 (1995).

482. WINN SCHARTAU, INFORMATION WARFARE 86 (1994). Some bombs are designed to explode at a predetermined altitude, others are set to explode only after penetrating a structure or digging themselves into the ground. Some explosive projectiles are designed to be armor piercing; others for anti-personnel application throw concentrations of skin-piercing shrapnel. They all have a purpose...deploy a complex mixture of weapons systems each of which is apropos to the circumstances. *Id.*

and the neutral world.[483] Similarly, in the information age, an enemy can target the information infrastructure to help in effectively destroying the enemy's armed force.[484]

Justifying a cyberattack as an armed attack in this respect, however, seems to be inadequate, as any attack as long as a weapon is used would just amount to an armed attack. Certainly, the U.N. Charter did not envision the use of the right of self-defense against almost every attack with any weapon. It would thus appear that the justification of a cyberattack qualifying as an armed attack rests more logically in terms of its effects or consequences, as may be gleaned from the decision in Nicaragua.

B. Qualifying A Cyberattack as an Armed Attack Based on Its Effects/Consequences

As Greenberg concisely stated, "Attacks will be judged largely by their effects, rather than by their methods."[485] In evaluating the propriety of taking defensive action, it seems more useful to consider the legal consequences of a computer-generated action, rather than the mechanism used to launch the attack.[486] An armed attack exists when force is used by a State on a relatively large scale and with substantial effect.[487] An enemy State may use a computer virus, which does not physically destroy, but results in shutting down a nation's electric grid vital to both military and civilian purposes.[488] If the attack has a debilitating effect on national security or on vital national interests, the right to respond is greatly enhanced.[489]

The author therefore asserts that two kinds of cyberattacks, in terms of effects or consequences, would trigger the right of self-defense: (1) a cyberattack which results in massive destruction, as if carried out using conventional/physical weapons; and (2) an intrusive attack to gain military

483. Martin Libicki, *What is Information Warfare?* (Aug. 1995) (unpublished manuscript, on file with Center for Advanced Command Concepts and Technology, Institute for National Strategic Studies, National Defense University).

484. *See generally* George Stein, *Information Warfare*, AIRPOWER J. 32 (1995).

485. GREENBERG, *supra* note 430, at 32.

486. *Information Warfare as International Coercion*, *supra* note 5.

487. SIMMA, *supra* note 94, at 51. *See generally* Randelzhofer, *Use of Force*, 4 E.P.I.L. 271 (1982); *Nicaragua*, 1986 I.C.J. ¶ 195 (a closer look reveals that the Court focused on the effects of the attack to trigger self-defense).

488. To get an extensive overview on the different kinds and effects of viruses, *see* LARRY BOND, THE ENEMY WITHIN (1996); RALPH PETERS, THE WAR IN 2020 (1991).

489. SHARP, *supra* note 352, at 205-6.

(tactical) advantage over another State where a state of war does not yet exist between such States.

1. A cyberattack which results in massive destruction

It seems reasonable to qualify cyber-assaults that are sufficiently destructive as armed attacks.[490] In the case where the State-sponsored attack is directed against a vital computer system controlling critical infrastructure,[491] the damage is likely to be of such magnitude so as to qualify the attack as a use of armed force.[492] If the cyberattack shuts down another State's air traffic control system, or causes banking institutions, financial systems, and public utilities to collapse, and opens the floodgates of dams resulting in deaths and property damage, such an attack qualifies as an armed attack.[493]

This form of cyberattack triggers the victim-State's right to respond with force in self-defense under Article 51 of the U.N. Charter.[494]

As an exception to the prohibition against the use of force,[495] Article 51 of the Charter indicates that there are certain uses of force that will not contravene the prohibitions in Article 2(4).[496] This rule provides ultimate protection for State autonomy – no State may be threatened by another State's decision to use force.[497] Accordingly, to require a State to tolerate attacks on infrastructure critical to its security and/or economic well-being without resistance, on the grounds that peaceful means have not been exhausted, is not only absurd, but nullifies the right to self-defense.[498] The legal criterion for a permissible use of force is established once a cyberattack, attributable to a State, against infrastructure systems critical to the stability and security of the nation, resulting in massive damage, has taken place.[499]

490. *Information Warfare as International Coercion*, *supra* note 5.

491. *See* Stone, *supra* note 480.

492. *See* SHARP, *supra* note 352, at 138 ("[A]n activity not traditionally considered an armed attack [is] used in such a way that it becomes tantamount in effect to an armed attack will generally be considered an armed attack.").

493. *Information Warfare as International Coercion*, *supra* note 5.

494. *See* SHARP, *supra* note 352, at 36.

495. SIMMA, *supra* note 94, at 10.

496. HIGGINS, PROBLEMS AND PROCESSES, *supra* note 200, at 239.

497. Mary Ellen O' Connel, *Regulating the Use of Force in the 21st Century: The Continuing Importance of state Autonomy*, 36 COLUM. J. TRANSNAT'L L. 472, 475 (1997).

498. Oscar Schachter, *The Lawful Resort to Unilateral Use of Force*, 10 YALE J. INT'L L. 291, 292 (1985) [hereinafter Schachter, *The Lawful Resort*].

499. Aldrich, *War in the Information Age*, *supra* note 44, at 232.

This being the case, a government can respond to a cyberattack by using the same degree, although may be a different kind, of force.[500] If a State has been subjected to a foreign-instigated cyberattack and suffered physical, financial, and mortal harm, that government is not expected to tolerate events that destroy its national infrastructure.[501] It is reasonable that a government subjected to such a cyberattack should be permitted to respond immediately by taking action in self-defense.[502]

So, does the right of self-defense exist even if the cyberattack has taken place already?

The author submits that it does.

There is nothing in either the travaux preparatoires or the text of the Charter to justify the claim that self-defense is impermissible after an attack ends.[503] This assertion comes from a misunderstanding of the Caroline case,[504] which deals with anticipatory self-defense, a broader right than the immediate parameters of article 51.[505] In fact, international law lawfully sanctions armed reprisals which are in the exercise of self-defense.[506] The notion of self-defense in international law developed out of age-old notions of individual self-preservation.[507] Self-defense is not only a matter of right, but of duty.[508]

Be that as it may, the author is not unmindful, and is one with highly-qualified publicists in saying, that the immediacy of the self-defense measure indicates its necessity and reasonableness. This, the author does not dispute. Admittedly, the fact that any State may be allowed to retaliate does not translate to an illimitable right to act in self-defense since the responding

500. *See* Clark Arend, *International Law and the Recourse to Force: A Shift in Paradigms*, 27 STAN. J. INT'L L. 1, 14 (1990).

501. *Information Warfare as International Coercion*, *supra* note 5.

502. *Id.*

503. Thomas Franck, *Terrorism and the Right of Self-Defense*, 95 AM. J. INT'L L. 839, 840 (2001) [hereinafter Franck, *Terrorism*].

504. *See infra* discussion on anticipatory self-defense.

505. Martin Rotgoff and Edward Collins, Jr., *The Caroline Incident and the Development of International Law*, 16 BROOK. J. INT'L L. 493-527 (1990) (affirming a contemporary view of self-defense in the context of the threat's imminence).

506. Bowett, *Reprisals*, *supra* note 402.

507. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 175-221 (2d. 1994) [hereinafter DINSTEIN].

508. For the historical evolution of the right of self-defense, *see* HUGO GROTIUS, THE LAW OF WAR AND PEACE (1925).

State still needs to comply with two basic requirements in justifying its measure as lawful.

Notably, even in the cases of a cyberattack,[509] the exercise of the right to self-defense remains subject to the limitations of proportionality and necessity.[510] However, the response can be in the form of traditional military force, or a response in kind as long as they are proportional and necessary.[511]

a) Proportionality

Proportionality simply requires a rational relationship between the nature of the attack and the nature of the response.[512] Although the relationship need not approach precision, a nation subjected to a mere inadvertent intrusion into an important computer system, without anything else, may not be entitled to launch a strike on the offender-nation as the United Nations condemns as reprisals those defensive actions that greatly exceed the provocation.[513] The response to a cyberattack must strive to balance the damage it inflicts, especially to civilians, against the military objectives it aims to accomplish. Accordingly, a cyberattack against civilian healthcare facilities, resulting in death, would not be permissible as an act of self-defense if the prior attack was merely against the victim-State's financial institutions, disrupting banking business.

The response to an armed attack by a State is generally controlled by the severity of the initial use of force.[514] Proportionality applies both to whether a given level of cyberforce is appropriate as a response to a particular grievance (as part of the law of the use of force, jus ad bellum) and whether a given cyber-action is appropriate in light of its objectives and the damages/casualties that will result (as part of the law of armed conflict, jus in bello).[515] In short, the degree of forcible response by an attacked State must be proportionate to the force applied by the attacking State in the initial

509. *Information Warfare as International Coercion*, *supra* note 5.

510. U.N. CHARTER, art. 103; SHAW, *supra* note 125, at 787; SIMMA, *supra* note 94, at 1116-25; GOODRICH, *supra* note 403, at 614-17; U.S. DEP'T OF STATE, TREATIES IN FORCE 447 (1999).

511 *See* SHARP, *supra* note 352, at 38.

512. AKEHURST'S MODERN INTRODUCTION, *supra* note 182, at 224; *see* INTERNATIONAL LAW AND THE USE OF FORCE, *supra* note 438, at 261-264; SIMMA, *supra* note 94, at 677.

513. *See* the Security Council's discussion, 36 U.N. SCOR. (2285-2288 Mtgs.), U.N. Docs. S/PV 2285-88 (1981).

514. *See* Franck, *Terrorism*, supra note 503, at 840.

515. RESTATEMENT (THIRD), § 905.

attack.[516] To demonstrate, a cyber-generated effort to temporarily bring down a society's financial or banking infrastructure would be an appropriate response to a computer intrusion that also temporarily disrupted public telecommunications in the victim-State.

b) Necessity

The requirement of proportionality is linked[517] to the principle of necessity.[518] Proportionality lays down a requirement that a response to an attack be limited in intensity and magnitude to what is reasonably necessary to secure the permissible objectives of self-defense.[519] In this respect, necessity requires that a State undertake self-defense only as a last resort.[520] While proportionality requires that a State demonstrate that actions taken in response are not excessive to the attack directed against its territory, necessity dictates urgency and reasonableness. Self-defense fully accepts the right of the attacked State to deal with an armed attack to the extent necessary to eliminate the breach of territorial integrity.[521] Thus, the notion of necessity entails that the degree of cyber-force employed be limited in magnitude, intensity, and duration to that which is reasonably necessary to counter the attack posed against the target State.[522]

Some scholars would argue that the Information Age modifies the principles of proportionality and necessity considering that cyberattacks on military targets may cause civilian systems connected to those military systems to fail. This is not totally without merit. This is so because a virus fed into an adversary's military computer might inadvertently or otherwise enter into civilian systems. A cyberattack on military power facilities, defense-related munitions factories, pharmaceutical plants, or nuclear power plants could pose problems for society in general if the computer-generated failure of a facility leads to the release of toxic substances into the atmosphere. Certain publicists would say that the attacked State's response should be

516. Baker, *Terrorism and the Inherent Right of Self Defense (A Call to Amend Article 51 of the United Nations Charter*, 10 HOUS. J. INT'L L. 25, 47 (1987).

517. Schachter, *The Lawful Resort*, *supra* note 499, at 292.

518. *See generally* CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 95 (1993).

519. MCDOUGAL & FELICIANO, *supra* note 400, at 242.

520. U.N. CHARTER, art. 2(3).

521. Eugene Rostow, *The Legality of the International Use of Force By and From States*, 10 YALE J. INT'L L. 286, 289 (1985).

522. *See* Jennings, *The Caroline and McLeod Case*, 32 AM. J. INT'L L. 82 (1938); SIMMA, *supra* note 94, at 677; J. Hargrove, *The Nicaragua Judgment and the Future of the Law of Force and Self Defence*, 81 AM. J. INT'L L. 135, 136 (1987).

limited to what was originally intended – that of attacking the military component. Therefore, does the cyberage allow a State to respond within the larger context of the effects of the attack?

The author is more inclined to say that the attacked State is permitted to consider the inevitable consequences of the attack on civilian systems to determine the proportional and necessary response.

The answer to this issue boils down to whether the attacked State necessarily waives its rights to respond proportionately to the effects of the cyberattack on civilian targets if it purposefully integrates military facilities into its civilian systems. At first, the answer would seem in the affirmative. A State leaves its civilian computer-based communications systems vulnerable to a legitimate attack if that government allows both military and civilian systems to run on the same networks.[523]

The author asserts, however, that the attacked State does not waive its right to respond proportionately to a cyberattack merely by integrating its military and civilian systems on the same networks. It has been well accepted in international law that the responding State must adapt the magnitude of its counter-measures to the scale and effects of the armed attack.[524] The obligation is on any State to be cautious of its own military attacks. Knowing that these military systems are inevitably linked to civilian systems due to the nature of the Internet, a State should be liable for all the consequences of its attacks against such systems.[525]

To put the obligation on the attacked State would be unreasonable as any State is permitted to take advantage of modernization and development.[526] Clearly, the consequences on civilian systems should be considered in formulating the necessary response to the attack. Thus, the attacked State may respond in proportion to the effects of the cyberattack.

2. Outside a state of war, intrusive cyberattacks against strategic information allows a State to respond in self-defense if such intrusion leads to an imminent cyber attack.

What if the attack does not result in destruction, but in mere intrusion only?

523. *Information Warfare as International Coercion*, *supra* note 5.

524. DINSTEIN, *supra* note 508, at 220.

525. Chorzow Factory (Germany v. Poland), 1928 P.C.I.J. Series A, No. 17, at 47.

526. Bariloch Declaration, G.A. 50th Plen. Mtg., U.N. Doc.A/50/673 (1995).

In 1999, an FBI investigation code-named Moonlight Maze[527] revealed the most extensive, thus far, computer attack aimed at the U.S. Government. Hackers from Russia penetrated DOD computers for more than a year and stole vast amounts of sensitive information.[528] According to Pentagon and FBI officials, the Russian hacking was a state-sponsored Russian intelligence campaign to secure U.S. technology,[529] which targeted not just the DOD, but also the Department of Energy, NASA, military contractors, and military-linked civilian universities,[530] illustrating the vulnerability of even the most protected military computer systems.

In this case, the author submits that the attacked State may respond in self-defense depending on how the stolen information will be used in the immediate, or short-term, time. The author stresses that if the data are vital to national security, or public safety or welfare, and the intruder intends to use it strategically against the intruded State, that kind of data intrusion may be afforded special protections under the regime of self-defense.[531] For example, if a State attacks the computer databases of another State's defense or military department, and steals classified information related to troop locations, or secret codes needed to launch military instruments, such actions could trigger the right to self-defense, even though no immediate loss of life or destruction results, provided that the attacked State discovers that there is evidence to support that the perpetrators are planning future cyberattacks.[532] In such a case, it can be reasonably inferred that the computer intruders were engaged in an ongoing attack against the defense establishment of the intruded State.

527. The NIPC is the FBI unit responsible for coordinating the federal response to computer threats. President Clinton made the FBI the lead agency for protecting the nation's computer systems when he signed Presidential Decision Directive 63 on May 22, 1998.

528. During his testimony before a Senate subcommittee on technology and terrorism, Michael A. Vatis, Director of the FBI's NIPC, stated that 'the intrusions appear to have originated in Russia,' and that the intruders stole 'unclassified but still sensitive information about essentially defence technical research matters.'

529. Kimery, *The Russians Are Coming*, 3 (5) MILITARY INFORMATION TECHNOLOGY, *available online at* www.MIT-kmi.com (last visited Apr. 15, 2002).

530. Drogin, LOS ANGELES TIMES, Oct. 7, 1999, at A1.

531. *Information Warfare as International Coercion*, *supra* note 5.

532. *Id.*

Such an imminent threat triggers self-defense in anticipation of an armed attack.[533]

The use of the word "inherent" in the text of article 51 suggests that self-defense is broader than the immediate Charter parameters. The United States has long taken the position that each nation is free to defend itself and is the judge of what constitutes the right of self-defense and the necessity of the same.[534] Similarly, more than a half- century ago, Secretary of State Frank Kellogg noted that when a State has resorted to the use of force, if it has a good case, the world would applaud and not condemn its actions.[535] During the drafting of a related instrument, the Kellogg-Briand Treaty, the United States expressed its view on the right of self-defense as follows:

> There is nothing in the American draft of an anti-war treaty which restricts or impairs in any way the right of self-defense. That right is inherent in every sovereign state and is implicit in every treaty. Every nation is free at all times and regardless of treaty provisions to defend its territory from attack or invasion and it alone is competent to decide whether circumstances require recourse to war in self-defense.[536]

As self-defense is an inherent right,[537] its contours have been fashioned by customary international law, and are thus subject to customary interpretation. In practice, pro-active States have operationalized this broader right of self-defense through rules of engagement.[538]

533. *See* SIMMA, *supra* note 94, at 675. *See also* OPPENHEIM, *supra* note 59, at 421; CASSESE, *supra* note 453, at 230-3.

534. Brownlie, *The Use of Force*, *supra* note 454, at 207.

535. Secretary of State Kellogg, Address before the American Society of International Law, Apr. 28, 1928, *reprinted in* AM. SOC. INT'L L. PROC. 141, 143 (1928).

536. 5 MARJORIE WHITEMAN, DIGEST OF INTERNATIONAL LAW 971-72 (1965) [hereinafter WHITEMAN].

537. Walker, *Information Warfare*, *supra* note 2, at 1102.

538. UNITED STATES EXPLANATION OF VOTE AFTER THE VOTE *RE*: G.A. RES. 53/70 (1998), *reprinted in* SHARP, *supra* note 352, at 189. In the United States' context, this ensures that National Command Authorities' guidance for handling crisis responses to techno-violence and other threats is provided, through the Joint Chiefs of Staff, to subordinate headquarters and deployed U.S. forces both during armed conflict and in periods of crisis short of war. Rules of Engagement reflect domestic law requirements and U.S. commitments to international law. They are impacted by political, as well as operational considerations. For the commander concerned with responding to a threat to his communications/command and control infrastructure, these rules represent limitations or upper bounds on how to utilize defensive and/or responsive systems and forces, without diminishing the authority to effectively protect his own critical infrastructure from attack.

The final clause of article 2, paragraph 4, of the Charter supports this interpretation and forbids the threat or use of force "in any manner inconsistent with the Purposes of the United Nations."[539] This interpretation of the customary right of self-defense, as limited by the requirements of necessity and proportionality,[540] can scarcely be regarded as inconsistent with the purpose of the United Nations, and a decent respect for balance and effectiveness would suggest that a conception of impermissible coercion, which includes threats of force, should be countered with an equally comprehensive and adequate conception of permissible or defensive coercion.[541]

In any case, as Professor Lauterpacht has pointed out, every State judges for itself, in the first instance, whether a case of necessity in self-defense has arisen, but if later on its illegality is raised, such question is justiciable for an international judicial authority or political body.[542]

Under customary international law, the larger context of the right of self-defense is to be tested against the criteria enunciated in the Caroline Incident.[543] In 1837, British forces took action against Canadian insurgents who had mounted several attacks from islands in the Niagara River. The British sought to capture the U.S. steamboat Caroline that the rebels had chartered to maintain their supply lines. The British seized the Caroline while it was moored in U.S. territory, burned the vessel and sent it downstream where it plunged over the Falls. During the incursion, the British killed several U.S. citizens. The U.S. Government complained that its

Techno-violence against a critical U.S. computer system, whether information, communications, or command and control-related, represents hostile activity which may trigger the applicable ROE. Until June 1986, the only U.S. peacetime Rules of Engagement applicable worldwide were the JCS Peacetime ROE for U.S. Sea-borne Forces. These Rules, which until 1986 served as the basis for all commands' peacetime ROE, were designed exclusively for the maritime environment. In June 1986, Secretary of Defense Weinberger promulgated more comprehensive ROE for sea, air, and land operations worldwide. The 1986 Peacetime ROE provided the on-scene commander with the flexibility to respond to hostile intent as well as hostile acts and unconventional threats with minimum necessary force and to limit the scope and intensity of the threat. *See id.*

539. George Shultz, *Low Intensity Warfare: The Challenge of Ambiguity*, U.S. DEP'T STATE CURRENT POL'Y NO. 783, Jan. 1986, at 3.

540. Claude Humphrey Meredith Waldock, *The Regulation of Force by Individual States, in* INTERNATIONAL LAW, 81 RECUEIL DES COURS 451, 496-99 (1952)

541. Myres McDougal, *The Soviet-Cuban Quarantine and Self-Defense*, 57 AM. J. INT'L L. 597, 600 (1963).

542. *See* OPPENHEIM, *supra* note 59, at 299.

543. Caroline Case, 29 B.F.S.P. 1137-1138; 30 B.F.S.P. 195-196.

sovereignty had been breached by the British, who countered that they had simply acted in self-defense.[544] Rejecting Britain's invocation of self-defense, although recognizing the right of anticipatory self-defense,[545] the case pronounced:

> It had to be demonstrated that the need for self-defense was instant, overwhelming, leaving no choice of means, and no moment for deliberation. It was also necessary for Britain to show that the Canadian authorities had done nothing unreasonable or excessive; since the act, justified by the necessity of self-defense, must be limited by that necessity and kept clearly within it.[546]

This comprehensive conception of permissible or defensive actions, honoring appropriate response to threats of an imminent nature, is merely reflective of customary international law.[547] The broader test of whether a State has a right to respond in self-defense to an armed attack is the imminence of the attack, dating back to the Caroline Case, which has been identified as the principle of anticipatory self-defense.[548] The right of anticipatory self-defense exists even in the Charter era because extensive State practice through municipal legislation[549] and mutual defense treaties since 1945 have continued to allow measures constituting anticipatory self-defense.[550] The principle of anticipatory self-defense asserts that the use of force by one State against another is permissible in the event of imminent danger or an actual threat of armed attack.[551]

544. WALLACE, *supra* note 205, at 252.

545. Franck, *Terrorism*, *supra* note 504, at 840.

546. *Caroline*, 29 B.F.S.P. 1137-1138; 30 B.F.S.P. 195-196.

547. *See* Terry, *Responding to Attacks*, *supra* note 361, at 176.

548. *See* DINSTEIN, *supra* note 503, at 172. *See also* David K. Linnan, *Self-Defense, Necessity and U.N. Collective Security: United States and Other Views*, 1991 DUKE J. COMP. & INT'L L. 57, 65-84, 122 (1991); James McHugh, *Forcible Self-Help in International Law*, NAVAL WAR C. REV. at 61 (Nov.-Dec. 1972).

549. Richard J. Grunawalt, *The JCS Standing Rules of Engagement: A Judge Advocate's Primer*, 42 AIR FORCE L. REV. 245 (1997); J. Ashley Roach, Rules of Engagement, NAVAL WAR C. REV. at 46 (Jan.-Feb. 1983), *reprinted in* 14 SYRACUSE J. INT'L L. & COM. 865 (1988); Ivan Shearer, *Rules of Engagement and the Implementation of the Law of Naval Warfare*, 14 SYRACUSE J. INT'L L. & COM. 767 (1988).

550. *See* George K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said, in* THE LAW OF MILITARY OPERATIONS: LIBER AMICORUM PROFESSOR JACK GRUNAWALT 365, 379 (Michael N. Schmitt ed., 1998) [hereinafter Walker, *Anticipatory Collective Self-Defense*].

551. Walker, *Information Warfare*, *supra* note 2, at 1103.

The criterion, therefore, is that the threat must be real and credible to create an imminent need to act, with a genuine probability of attack.[552] The threat must be instant, and overwhelming, leaving no choice of means, and no moment for deliberation.[553] The reasonable conclusion is that international law is not a suicide pact among States, and thus a State does not have to wait until it is physically harmed to defend itself.[554] To reiterate, however, although the responding State may be allowed to invoke the right of anticipatory self-defense, it must establish that sufficient proof exists about any planned attack as a result of the information stolen initially.

Applying the principle in the cyberage, it is precisely this anticipatory element that is critical to an effective policy to counter intrusive acts against critical information systems.[555] This is important because the only credible response to attacks on critical infrastructure is deterrence.[556] Where there is evidence that a continuation of intrusive electronic sabotage will occur in order to attack the State, a response beyond the initial intrusion would be legally appropriate to counter the continuing threat.[557] It would be unreasonable to preclude the victim of techno-violence from redress, based upon a determination that the initial threat of the intrusion into a critical system is no longer imminent, when the perpetrator's own actions have precluded immediate identification.[558]

According to general legal rules for self-defense, therefore, not only may a government respond to an attack already launched against its territory, but a government can also take self-defensive military action in anticipation of an armed attack[559] by virtue of a cyber-intrusion. If applied to the Moonlight

552. Horwitz, *The Tokyo Trial*, 465 INT'L CONC. 560 (1950).

553. *See The Caroline Case*, *in* J.B. MOORE, II DIGEST OF INTERNATIONAL LAW 409 (1906). BOWETT, SELF-DEFENCE, *supra* note 438, at 59; R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AM. J. INT'L L. 89 (1938).

554. U.N. CHARTER, art. 51. *See* George K. Walker, *Anticipating Collective Self-Defense in the Charter Era: What the Treaties Have Said*, 31 CORNELL INT'L L.J. 321, 347 (1998). *See also* Walker, *Anticipatory Collective Self-Defense*, *supra* note 551.

555. *See generally* Brian A. Persico, *Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure*, 7 COMM. L. CONSPECTUS 153, 156-60 (1999). The author discusses how an attack against critical infrastructure would have a debilitating effect on U.S. defense or economic security.

556. Terry, *Responding to Attacks*, *supra* note 361, at 184.

557. *Id.* at 177-8.

558. *Id.* at 177.

559. Letter from Secretary Webster to Mr. Fox, dated Apr. 24, 1981, *reprinted in* BRITISH AND FOREIGN STATE PAPERS 1129, 1138 (1857). The traditional principle of anticipatory self-defense was first enunciated by Secretary of State Daniel Webster in his response to a Canadian attack on the American ship *Caroline*, which has been assisting Canadian rebels in their efforts against the Canadian Government.

Maze situation, the U.S. could only lawfully act in anticipatory self-defense against Russia if the U.S. had established that another Russian attack was imminent.

Ultimately, the effects of cyberattacks call for a more practical approach to dealing with cyberattacks, one which would tolerate the pre-emptive use of cyberforce under the doctrine of anticipatory self-defense – when a government perceives that there exists a significant and real threat to its national security, and responds to pre-empt that threat in a proportionate and necessary manner without any alternative.[560] To be eventually adjudged as lawful, the response in anticipatory self-defense to counter cyberattacks would rest upon the ability to determine the reality of the perceived threat and the reasonableness of the response in self-defense, and which would have to meet both a subjective and an objective test.

While the subjective test would ascertain whether the purported target-State had reasonable grounds to believe that a real threat existed, the objective test would determine whether third-party States viewed the threat in the same light.[561] When applied to the transnational use of cyber-force, anticipatory self-defense would allow governments to meet their minimum national security requirements and at the same time ensure that the use of force is necessary and proportional under the circumstances.

For over a century, the legal theories drawn from the Caroline incident have influenced the interpretation of international legal rules, in respect of the inherent right of self-defense. While a formal international instrument is still lacking to substantiate the applicability of anticipatory self-defense as a universally accepted principle of international law, no consensus actively opposes the concept either.[562] Lack of opposition is significant in the formation of a customary rule; otherwise put, sufficient State practice precludes the development of a customary norm[563] against anticipatory self-defense. It thus appears that no strict prohibition precludes a government using cyber-force preemptively as long as the perceived threat is

560. George K. Walker, *Maritime Neutrality in the Charter Era*, 17 CENTER OCEANS L. & POL'Y PROC. 124, 142-4 (1993).

561. *See generally* MCDOUGAL & FLORENTINO FELICIANO, *supra* note 400.

562. Franck, *Terrorism*, *supra* note 504, at 840; *Information Warfare as International Coercion*, *supra* note 5; SHARP, *supra* note 352, at 33-48. Sharp says that the real debate is the scope of the anticipatory self-defense right and that responses must be proportional.

563. HARRIS, CASES AND MATERIALS, *supra* note 1, at 43. *See* HIGGINS, PROBLEMS AND PROCESSES, *supra* note 200, at 23.

demonstrated to be real and immediate, and the criteria of proportionality and necessity as general legal rules are adhered to in the application of computer-generated intrusion.[564]

To recapitulate, the right of self-defense may be necessary, either: (1) to immediately defend that State by reacting to a cyberattack against critical infrastructure that already occurred; or (2) to prevent future attacks after an initial intrusion into vital computer systems has taken place, provided that the attack is actual or the threat is imminent and without any alternative choice of means. In both cases, the victim-State may lawfully invoke self-defense to justify reasonable, necessary, and proportional measures to safeguard its security. This, in essence, embodies the right of self-defense.[565]

C. In a Case Where the Attacks do not Constitute Armed Attacks but are Evidently Continuing, the attacked State is not precluded from taking countermeasures against the attacking State.

According to Article 22 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts,[566] the wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State.[567] The Commentary of the International Law Commission has included reprisals in this broader response to a wrongful act.[568] The attacked State may respond with reprisals not involving use of force,[569] or retorsions under the necessity doctrine.[570]

564. *See Information Warfare as International Coercion, supra* note 5.

565. W. O'BRIEN, THE LAW OF LIMITED INTERNATIONAL CONFLICT 23-32 (1965); BOWETT, SELF-DEFENCE, *supra* note 438, at 269.

566. Draft Articles, adopted by the ILC at its 53rd Session (2001), Report of the I.L.C. on the Work of its 53rd Session, U.N. GAOR, 56th Sess., Supp. No. 10 (A/56/10), art. 21 (2001).

567. Draft Articles, art. 22.

568. Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the ILC at its 53rd Session (2001), Extract from the Report of the ILC on the Work of its 53rd Sess., U.N. GAOR, Supp. No. 10 *A/56/10, Ch. IV.E.2, 120-122 (2001) *also available at* http://www.un.org/law/ilc/texts/state_responsibilty/responsibility_commentaries [hereinafter Commentaries to the Draft Articles]

569. According to Article 50:

1. Countermeasures shall not affect:

(a) The obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations;

(b) Obligations for the protection of fundamental human rights;

A reprisal allows a State to commit an act that would otherwise be illegal to counter the illegal act of another State.[571] However, armed reprisals are still prohibited, unless they are exercised by virtue of the right of self-defense.[572]

An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce the latter State to comply with its obligations, which must be limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State.[573] However, countermeasures must be commensurate to the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.[574]

The injured State, before taking such measures, must call on the responsible State to fulfill its obligations and notify the responsible State of any decision to take countermeasures and offer to negotiate with that State, unless such measures are urgent and necessary to preserve its rights.[575] Therefore, a cyberattacked State may respond in some other form of countermeasures, not involving the use of force, to require the party to cease its wrongful conduct.

After having evaluated both individual and State-sponsored cyberattacks, what, precisely, are the lawful remedies available to the attacked State in order to respond to varying degrees of cyberattacks? This shall be discussed in the next Chapter.

(c) Obligations of a humanitarian character prohibiting reprisals;

(d) Other obligations under peremptory norms of general international law.

2. A State taking countermeasures is not relieved from fulfilling its obligations:

(a) Under any dispute settlement procedure applicable between it and the responsible State;

(b) To respect the inviolability of diplomatic or consular agents, premises, archives and documents.

570. Walker, *Information Warfare, supra* note 2.

571. Terry, *Responding to Attacks, supra* note 361, at 174-5.

572. Bowett, *Reprisals, supra* note 402.

573. Draft Articles, art. 50.

574. *Id.* art. 51.

575. *Id.* art. 52.

VI. ESTABLISHING THE APPROPRIATE RESPONSES UNDER INTERNATIONAL LAW TO VARYING DEGREES OF CYBERATTACKS

After evaluating varying degrees of cyberattacks, from simple hacking to cyberterrorism to cyber-use of force, it is now necessary to discuss the appropriate response to each form of cyberactivity,[576] as a prior illegal act has an equivalent responsibility under international law.[577] As new technologies generate enhanced vulnerabilities, the appropriate response to a cyberattack must be regarded seriously - not merely to know when a cyber-based attack might occur, but more critically, to know how to react appropriately if such a cyberattack occurs.[578]

As discussed in the preceding chapters, to the extent the attack was caused by an individual, the response would likely be limited to criminal prosecution, but if it can be ascertained that a foreign country orchestrated the takedown, a State may be entitled to respond proportionately under the right of self-defense.[579] However, in the latter case, State Responsibility would again depend on varying degrees of participation. The response of an attacked State against a State sponsoring a cyberattack should differ from that of a State aiding or abetting the same, or from a State harboring a cyberterrorist. Apart from these considerations, the ways and means of capturing a cyberterrorist would be restricted by certain norms under international human rights law.

This Chapter shall delineate the levels of responses proportional and necessary to corresponding levels of cyberattacks, from mere hacking activities to cyberterrorism to cyber-use of force.

A. Responding to Attacks by Individuals

1. Activism: No Prosecution

Activism cannot be criminalized without any limitation as any information dissemination over the Internet is protected by the fundamental right of freedom of expression, which includes the right to receive and impart information in whatever medium.[580] International law, however, permits

576. Creekman, *Response to China*, *supra* note 431, at 655.

577. Draft Articles, art. 1.

578. George Shultz, Address before the Low Intensity Warfare Conference, National Defense University, Washington, D.C. (Jan. 15, 1986).

579. Aldrich, *War in the Information Age*, *supra* note 44, at 232.

580. Universal Declaration of Human Rights (UDHR), art. 19, G.A. Res. 217 (III 1948); European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), art. 10, 312 U.N.T.S. 221 (1950); African Charter on Human and People's Rights (African Charter), arts. 9 & 10, *reprinted*

restrictions on free speech for the protection of national security or of public order or of public health and morals,[581] such as racist speech.[582] Thus, a State cannot totally prohibit the use of computer systems for purposes of mere activism, without more.[583]

2. Hactivism: Domestic Prosecution

A State retains jurisdiction over crimes committed or felt within its territory,[584] or serious crimes against its own safety.[585] The objective territorial principle[586] grants a State jurisdiction when the crime is consummated or its effects felt in the State's territory,[587] regardless of the victim's and the perpetrator's nationalities.[588] Thus, the appropriate response to such acts would be prosecution under municipal law pursuant to the objective territoriality principle. For example, the "Melissa Virus" disrupted e-mail service around the world when it was posted to an Internet newsgroup in 1999 affecting more than 100,000 users world-wide.[589] The man accused of creating the "Melissa Virus" was charged with violating New Jersey computer laws, including interruption of public communication, theft of computer services, and damage or wrongful access to computer systems.[590] As such, the responsibility of an individual shall be dealt with by

in 21 I.L.M. 58 (1982); American Declaration on the Rights and Duties of Man (American Declaration), art. 4, OAS Res. XXX, OEA/Ser.L.V/II.82.doc.6.rev.1 (1992).

581. International Covenant on Civil and Political Rights (ICCPR), art. 19, G.A. Res. 2200 (XXI), U.N. GAOR 21st Sess., Supp. No. 16 at 52, U.N. Doc. A/6316 (1966).

582. GREWLICH, GOVERNANCE IN "CYBERSPACE": ACCESS AND PUBLIC INTEREST IN GLOBAL COMMUNICATIONS 290 (1999).

583. SCHWARTAU, *supra* note 28, at 407.

584. BROWNLIE, INTERNATIONAL LAW, *supra* note 186, at 300.

585. D.J. HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW 269 (4d. 1991).

586. WALLACE, *supra* note 205, at 112-113.

587. Wade Estey, *The Five Bases of Extraterritorial Jurisdiction and the Failure of the Presumption Against Extraterritoriality*, 21 HASTINGS INT'L & COMP. L. REV. 186 (1997). *See* United States v. Aluminum Co. of Am., 148 F.2d 416 (2nd Cir. 1945); WALLACE, *supra* note 205, at 113.

588 BROWNLIE, INTERNATIONAL LAW, *supra* note 186, at 303.

589. *See* Dean Takahashi, *Hackers Square Off Against Trackers In Long Battle Over Computer Viruses*, WALL ST. J., Apr. 2, 1999, at B2 (discussing efforts by computer-security experts to track virus writers).

590. *See E-Mail-Virus Suspect Faces State Charges*, CHI.. TRIB., Apr. 9, 1999, at 18.

domestic law enforcement;[591] hence, a private citizen responsible for hacking shall be prosecuted under a domestic hacking law.[592]

Aside from the objective territoriality principle, a State may also invoke the nationality theory[593] in prosecuting the perpetrator when the latter is a national of the same State, and commits the hacking crime abroad.

The Philippine experience with the "I love you" virus demonstrates this trend of criminalizing, municipally, the sending of a virus and other cybercrimes. After reviewing the investigation by the National Bureau of Investigation of the sending of the virus, the 11th Congress of the Philippines and the Senate started reviewing pending bills in the year 2000, and on June 14 of the same year, Republic Act No. 8792,[594] entitled, "An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions, Penalties for Unlawful Use Thereof and Other Purposes" (the E-Commerce Act), was passed.[595] Therefore, if an individual commits a hacking crime within Philippine territory, such criminal shall be prosecuted under the E-Commerce Act under the objective territoriality principle.[596]

What if the foreigner did not perform the act in Philippine territory, but abroad, and its effects were felt here? Under the objective territoriality principle, the Philippines can prosecute the hacker under the E-Commerce

591. DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 1973 (Rovine ed., 1974).

592. *See* Wong, *supra* note 365.

593. HARRIS, *supra* note 1, at 266.

594. R.A. 8792, An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions, Penalties for Unlawful Use Thereof and Other Purposes (2000).

595. *Cyber Attacks – War Without Borders: Hearings before the U.S. House Government Reform Subcommittee on Government Management, Information and Technology* (Jul. 26, 2000). Even the US investigated the Iloveyou virus incident. Chairman Horn and Mr. Spotila discussed that in varying degrees, all national agencies have sought to comply in developing an incident response capability and that all agencies are participating in the sharing of information on cyber threats and vulnerabilities.

596. Caesar Mañalac, a former information technology support head of a business school in the Philippines, is the first person to be prosecuted under the country's two year-old electronic commerce law. Philippine anti-fraud agents detained him on charges of violating the e-commerce law and qualified theft after raiding his house. The suspect is accused of having illegally accessed the system network of a school for the purpose of copying confidential files. *See* Agence France-Presse, *Philippines Hacker Arrested in Industry First*, May 5, 2002, *available at* http://www.techreview.com/offthewire/3001_352002_1.asp (last visited May 20, 2002).

act since the effects of the hacking were felt here. However, under the objective territoriality principle, the hacker could conceivably be prosecuted in every country where his hacking's effects were felt. Currently, it is possible that two or more, or even all, States will claim jurisdiction over the crime where its effects were felt. Thus, in the last Chapter, the author will offer some recommendations to address the jurisdictional quandary.

At present, would the State who has failed to prosecute these ordinary hackers have any responsibility under International Law?

Responsibility under International Law is not based upon delict in the municipal sense but requires a breach of a legal duty under treaty or an international custom. [597] However, although certain cyberattacks are criminalized in most States under recent legislation,[598] such practice does not constitute customary international law unless these States have legislated virtually in the same manner, as held in the case of the Scotia Vessel.[599] The formation of a custom requires, at least, substantial uniformity in State practice. [600] However, these pieces of legislation lack even substantial uniformity as to enforcement and punishment.[601] In fact, the discrepancy owing to the difference in these pieces of municipal legislation might create a problem in terms of extradition.[602] For instance, the European Union has a set of omnibus data protection laws, while the U.S. has none.[603] The U.K.'s legal system of prosecuting hacking differs from that of the United States and

597. *Chorzow*, P.C.I.J. Ser. A, no. 9, at 21.

598. *See* United States, Computer Fraud and Abuse Act, 18 U.S.C. §1030(1994); EU, Directive on the Protection of Individuals with Regard to the Processing of Data and on the Free Movement of Such Data, Directive 95/46 (1995); United Kingdom, Computer Misuse Act (1990); Philippines, E-Commerce Act (2000); Australia, CyberCrime Act (2001); Japan, Unauthorized Computer Access Law (1999); China, Protective Legislation of Computer Information System Security (2001); Taiwan, Computer Processing Personal Information Protection Law (1995); Korea, Information Communication Act (1999); Malaysia, Computer Crimes Act (1997); Singapore, Computer Misuse Act (1993); India, Information Technology Act (2000). *See generally* Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 STA. CLARA COMP. & HIGH TECH. L.J. 403, 417 (1996); McCausland, *Regulating Compute Crime*, *supra* note 213, at 501.

599. *See* Scotia Case, *cited in* 14 WALLACE 170 (1871).

600. Anglo-Norwegian Fisheries Case (U.K. v. Norway), 1951 I.C.J. 116, at 131.

601. Soma, *Transnational Extradition*, *supra* note 331, at 333. *See* Peritt, Jr., *Jurisdiction in Cyberspace*, *supra* note 1, at 126-17.

602. Soma, *Transnational Extradition*, *supra* note 331, at 346.

603. *See* Mayer-Schoenberger, *The Internet and Privacy Legislation: Cookies for a Treat?* 1 W. VA. J. L. & TECH. 1, 4 (1997) [hereinafter *The Internet and Privacy Legislation*].

Canada in that its domestic system is not as strong in attacking the ends of hacking.[604]

Although there are existing guidelines issued by the Organization for the Economic Cooperation and Development,[605] the International Chamber of Commerce,[606] and The Eight,[607] these guidelines are not in themselves sources of international obligations and only constitute what is termed as soft law or de lege ferenda[608] – those rules which allow a State to relate to the law as it should be if the rules were changed to accord with good policy.

At present, the only treaty that exists which specifically deals with computer crimes is the European Convention on Cybercrime,[609] which has not entered into force as not a single State party has ratified the treaty as of 14 July 2002. Further, this treaty has been criticized for not representing and defining the common interests of the international community.[610] Currently, there are 32 signatories, with 28 being member-States of the Council of Europe. Only four (4) non-member States of the Council of Europe have signed the treaty.[611] In fact, the Philippines is not a party to said treaty. Therefore, unless the State is a party to the Convention, no treaty obligation is binding on any State. Beyond treaty law, no specific rules directly punish States for failing to actively suppress hacking per se.[612]

What the opinio juris of States seems to reflect is the duty to prevent hacking that constitutes cyberterrorism.[613]

604. Robert Sciglimpagia, Jr., *Computer Hacking*, 3 PACE Y.B. INT'L L. 199, 234 (2001) [hereinafter *Computer Hacking*].

605. O.E.C.D. GUIDELINES, *supra* note 159; O.E.C.D. COMPUTER RELATED CRIME, *supra* note 159.

606. INTERNATIONAL CHAMBER OF COMMERCE REPORT, COMMISSION ON COMPUTING, TELECOMMUNICATIONS AND INFORMATION POLICIES, COMPUTER-RELATED CRIME: AN INTERNATIONAL BUSINESS VIEW (1988).

607. MEETING OF THE EIGHT, *supra* note 222.

608. BROWNLIE, INTERNATIONAL LAW, *supra* note 186, glossary.

609. DRAFT CONVENTION ON CYBERCRIME, FINAL ACTIVITY REPORT, COMMITTEE OF EXPERTS ON CRIME IN CYBERSPACE (2001); Pounder, *The Council of Europe Cyber-Crime Convention*, 20 COMP. & SECURITY 380 (2001).

610. *Cybercrime Convention*, E-COMMERCE NEWS, Jun. 30, 2001, at 1.

611. These States are Canada, Japan, South Africa, and the United States.

612. *Computer Hacking*, *supra* note 605, at 210. *See The Internet and Privacy Legislation*, *supra* note 604.

613. G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc.A/RES/53/70 (1998); Pollitt, *Fact or Fancy?*, *supra* note 33, at 285-289.

3. Cyberterrorism: Universal Jurisdiction

As substantiated by individual and collective State practice, cyberterrorism can be defined as the politically motivated attack, through the use of computers and against computers controlling critical infrastructure, resulting in violence or serious economic hardship to civilians or non-combatants, generating a state of terror in the minds of the general public.[614] Cyberterrorism is simply a variant of terrorism – catastrophic terrorism,[615] and as every State is obliged to suppress terrorism,[616] all States are bound to prosecute terrorists regardless of the methods and practices used.[617] As customary law imposes a duty on States to take all necessary and effective measures to prevent and eliminate terrorism,[618] a State should be on the look-out for any national or resident involved in a cyberterrorist activity as any terrorist act is wrongful, regardless of the means employed,[619] such as the Internet.[620]

614. *See supra* notes 307-11 and accompanying text.

615. *See* Barry Kellman & David Gualtieri, *Barricading the Nuclear Window – A Legal Regime to Curtail Nuclear Smuggling*, 1996 U. ILL. L. REV. 667, 667-9 (1996)

616. S.C. Res. 1368, U.N. Doc.S/RES/1368 (2001); S.C. Res. 1373, U.N. Doc.S/RES/1373 (2001). *See* Michael Reisman, *In Defense of World Public Order*, 95 AM. J. INT'L L. 833, 833 (2001); Franck, *Terrorism*, *supra* note 504.

617. Michael Reisman, *International Legal Response to Terrorism*, 22 HOUS. J. INT'L L. 3, 41-54 (1999). *See* G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc.A/RES/53/70 (1998); G.A. Res. 3034, U.N. GAOR, 27th Sess., Supp. No. 30, at 1, U.N. Doc. A/RES/3034 (XXVII) (1973); G.A. Res. 31/102, U.N. GAOR, 31st Sess., Agenda Item 113, at 1, U.N. Doc. A/RES/102 (1976); G.A. Res. 34/145, U.N. GAOR, 34th Sess., Agenda Item 112, ¶ 3, at 2, U.N. Doc. A/RES/145 (1980); G.A. Res. 32/147, U.N. GAOR. 32nd Sess., Agenda Item 118, at 1, U.N. Doc. A/RES/147 (1978); G.A. Res. 36/109, U.N. GAOR, 36th Sess., Agenda 114, pmbl., at 2, U.N. Doc. A/RES/36/109 (1981).

618. Address to the Nation Announcing Strikes Again Al Qaida Training Camps and Taliban Military Installations in Afghanistan, 37 WEEKLY COMP. PRES. DOC. 1432, 1432 (2001). *See* European Convention on the Suppression of Terrorism, *supra* note 102; Organization of African Unity, Draft Convention of the Organization of African Unity on the Prevention and Combating of Terrorism, CAB/LEG/24.14/Vol.I/Rev.3 (1999); Conference on Combatting International Terrorism, *supra* note 129; Member States of the South Asian Association for Regional Cooperation, Regional Convention on Suppression of Terrorism, U.N. GAOR, 6th Comm., 44th Sess., U.N. Doc. A/51/136(1989). *See Legal Aspects of International Political Relations*, U.N.Y.B. 1063-65 (1987).

619. *Ascertaining* Opinio Juris, *supra* note 73, 323. *See* G.A. Res. 40/61, U.N. GAOR, 40th Sess., Agenda Item 129, at 3, U.N. Doc. A/RES/40/61 (1985); G.A. Res. 42/159, U.N. GAOR, 42nd Sess., Agenda Item 126, at 1, U.N. Doc. A/RES/42/150 (1987); G.A. Res. 46/51, U.N. GAOR, 46th Sess., Agenda Item 125, at 4, U.N. Doc. A/RES/46/51 (1991). *See generally* CHARLES

The international impact of cyberterrorist acts makes it an international crime that triggers universal jurisdiction.[621] The universality principle permits jurisdiction over crimes that are universally offensive[622] and universally punished because of the extreme horror that they evoke.[623] The principle of universality is widely accepted for specific breaches of an international character, specifically in the area of terrorism; hence because terrorism threatens the very nature of humanity itself, every nation has the right, and the duty, to prosecute these crimes and prevent their recurrence.[624]

Therefore, if a State has knowledge of any cyberterrorist activity, it is obliged to prosecute the perpetrator or, at the very least, exercise due diligence in ascertaining whether such criminal can be located within its territory.[625] If the perpetrator simply fled into another State, that State is still obliged to exercise the same degree of diligence.

The problem, however, is that the Philippines as of now has not passed any law relating to terrorism and cyberterrorism. Some scholars argue that a law is needed even with respect to crimes triggering universal jurisdiction. This is bolstered by the fact that even Piracy, a crime hostes humanis generis, is still punishable under the Revised Penal Code of the Philippines[626] even if

DUNLAP, TECHNOLOGY AND THE 21ST CENTURY BATTLEFIELD: RECOMPLICATING MORAL LIFE FOR THE STATESMAN AND THE SOLDIER 1-19 (1999).

620. *See* Bruce Hoffman, Responding to Terrorism Across the Technological Spectrum *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 3339, 339-67 (John Arquilla & David Ronfeldt eds., 1997).

621. *See Invoking State Responsibility*, *supra* note 60, at 4. *See also* Goodwin-Gill, *Crime in International Law: Obligations* Erga Omnes *and the Duty to Prosecute*, *in* THE REALITY OF INTERNATIONAL LAW: ESSAYS IN HONOUR OF IAN BROWNLIE 207 (Goodwin-Gill & Talmon eds., 1999) [hereinafter Goodwin-Gill].

622. *See* Demjanjuk v. Petrovsky, 776 F.2d 571, 582 (6th Cir. 1985). Some crimes are so universally condemned that the perpetrators are the enemies of all people, and that any nation which has custody of the perpetrators may punish them according to its law.

623. *See* Beverly Izes, Note, *Drawing Lines in the Sand: When State-Sanctioned Abductions of War Criminals Should Be Permitted*, 31 COL. J. L. & SOC. PROB.1, 11 (1997).

624. *See id.*

625. Orentlicher, *Settling Accounts: The Duty to Prosecute Human Rights Violations of a Prior Regime*, 100 YALE L.J. 2537, 2569-76 (1991)

626. Act No. 3815, An Act Revising the Penal Code and Other Penal Laws [REVISED PENAL CODE], art. 122-3 (1930).

> Art. 122. Piracy in general and mutiny on the high seas. — The penalty of reclusion temporal shall be inflicted upon any person who, on the high seas, shall attack or seize a vessel or, not being a member of its complement nor a passenger, shall seize the whole or part of the cargo of said vessel, its equipment, or personal belongings of its complement or passengers.
>
> The same penalty shall be inflicted in case of mutiny on the high seas.
>
> Art. 123. Qualified piracy. — The penalty of reclusion temporal to death shall be imposed upon those who commit any of the crimes referred to in the preceding article, under any of the following circumstances:
>
> 1. Whenever they have seized a vessel by boarding or firing upon the same;
>
> 2. Whenever the pirates have abandoned their victims without means of saving themselves; or
>
> 3. Whenever the crime is accompanied by murder, homicide physical injuries or rape.

jurisdiction is universally conferred. Fortunately, House Bill 3802[627] was proposed. However, the definition found therein stated:

> ...[U]nauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents.[628]

This definition, however, falls short of the definition that the author has culled from the practice of other States. With the definition proposed by House Bill 3802, any and all cyberactivities where intrusion is a result or an objective may be classified as cyberterrorism under Philippine law. Although the bill sufficiently covers the means employed, it does not include the other elements of cyberterrorism under present international norms. It must be emphasized that cyberterrorism remains a category of its mother concept – terrorism. As such, the element of intent to cause serious harm to civilians, resulting terror in the general public and the political motive must be addressed by the bill. A crime, especially a universal one, must be defined in accordance with how other States define it. Therefore, the author shall recommend an amendment to House Bill 3802, instead of proposing a new law, to prevent duplicity and superfluity.

627. H.B. 3802, 12th Cong. (1st Regular Sess. 2001).

628. *Id.* § 3(i).

The international impact of cyberterrorist acts makes it an international crime that triggers universal jurisdiction.[621] The universality principle permits jurisdiction over crimes that are universally offensive[622] and universally punished because of the extreme horror that they evoke.[623] The principle of universality is widely accepted for specific breaches of an international character, specifically in the area of terrorism; hence because terrorism threatens the very nature of humanity itself, every nation has the right, and the duty, to prosecute these crimes and prevent their recurrence.[624]

Therefore, if a State has knowledge of any cyberterrorist activity, it is obliged to prosecute the perpetrator or, at the very least, exercise due diligence in ascertaining whether such criminal can be located within its territory.[625] If the perpetrator simply fled into another State, that State is still obliged to exercise the same degree of diligence.

The problem, however, is that the Philippines as of now has not passed any law relating to terrorism and cyberterrorism. Some scholars argue that a law is needed even with respect to crimes triggering universal jurisdiction. This is bolstered by the fact that even Piracy, a crime hostes humanis generis, is still punishable under the Revised Penal Code of the Philippines[626] even if

DUNLAP, TECHNOLOGY AND THE 21ST CENTURY BATTLEFIELD: RECOMPLICATING MORAL LIFE FOR THE STATESMAN AND THE SOLDIER 1-19 (1999).

620. *See* Bruce Hoffman, Responding to Terrorism Across the Technological Spectrum *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 3339, 339-67 (John Arquilla & David Ronfeldt eds., 1997).

621. *See Invoking State Responsibility*, *supra* note 60, at 4. *See also* Goodwin-Gill, *Crime in International Law: Obligations* Erga Omnes *and the Duty to Prosecute*, *in* THE REALITY OF INTERNATIONAL LAW: ESSAYS IN HONOUR OF IAN BROWNLIE 207 (Goodwin-Gill & Talmon eds., 1999) [hereinafter Goodwin-Gill].

622. *See* Demjanjuk v. Petrovsky, 776 F.2d 571, 582 (6th Cir. 1985). Some crimes are so universally condemned that the perpetrators are the enemies of all people, and that any nation which has custody of the perpetrators may punish them according to its law.

623. *See* Beverly Izes, Note, *Drawing Lines in the Sand: When State-Sanctioned Abductions of War Criminals Should Be Permitted*, 31 COL. J. L. & SOC. PROB. 1, 11 (1997).

624. *See id.*

625. Orentlicher, *Settling Accounts: The Duty to Prosecute Human Rights Violations of a Prior Regime*, 100 YALE L.J. 2537, 2569-76 (1991)

626. Act No. 3815, An Act Revising the Penal Code and Other Penal Laws [REVISED PENAL CODE], art. 122-3 (1930).

> Art. 122. Piracy in general and mutiny on the high seas. — The penalty of reclusion temporal shall be inflicted upon any person who, on the high seas, shall attack or seize a vessel or, not being a member of its complement nor a passenger, shall seize the whole or part of the cargo of said vessel, its equipment, or personal belongings of its complement or passengers.
>
> The same penalty shall be inflicted in case of mutiny on the high seas.
>
> Art. 123. Qualified piracy. — The penalty of reclusion temporal to death shall be imposed upon those who commit any of the crimes referred to in the preceding article, under any of the following circumstances:
>
> 1. Whenever they have seized a vessel by boarding or firing upon the same;
>
> 2. Whenever the pirates have abandoned their victims without means of saving themselves; or
>
> 3. Whenever the crime is accompanied by murder, homicide physical injuries or rape.

jurisdiction is universally conferred. Fortunately, House Bill 3802[627] was proposed. However, the definition found therein stated:

> ...[U]nauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents.[628]

This definition, however, falls short of the definition that the author has culled from the practice of other States. With the definition proposed by House Bill 3802, any and all cyberactivities where intrusion is a result or an objective may be classified as cyberterrorism under Philippine law. Although the bill sufficiently covers the means employed, it does not include the other elements of cyberterrorism under present international norms. It must be emphasized that cyberterrorism remains a category of its mother concept – terrorism. As such, the element of intent to cause serious harm to civilians, resulting terror in the general public and the political motive must be addressed by the bill. A crime, especially a universal one, must be defined in accordance with how other States define it. Therefore, the author shall recommend an amendment to House Bill 3802, instead of proposing a new law, to prevent duplicity and superfluity.

627. H.B. 3802, 12th Cong. (1st Regular Sess. 2001).

628. *Id.* § 3(i).

B. Responding to Attacks with State Participation

1. Preparatory Stage

The participation of a State in the preparatory stage of a cyberattack can be direct or indirect. The responsibility of the State and the response to such a wrongful act shall differ depending on the level of participation of the State.

a) Direct Involvement

A State can be directly involved in the act of an individual if it is conducted by the State's governmental authorities or its organ, or by the State's instructions or control.[629] If a cyberattack was State-sponsored, the attacked State may lawfully act in self-defense[630] against the attacking State, as previously discussed.[631] By treating cyber-terrorists as participants in international coercion where a clear linkage can be tied to a State actor, the right of self-defense against their sponsor is triggered, and the use of force may be the only proportional response to the threat.[632] This pro-active strategy to the threat posed by attacks on critical infrastructure embraces the use of proportional protective, defensive, non-military, and military measures against the attack.[633] Thus, in this case, and subject to the two kinds of cyberattacks mentioned in the last Chapter (cyberattacks resulting in massive destruction and intrusive cyberattacks leading to an imminent cyberattack), the right of self-defense may be invoked.

As an alternative, the attacked State is not precluded from suing the attacking State before the International Court of Justice to require the latter to comply with the obligation breached,[634] to cease the wrongful act, and offer appropriate assurances and guarantees of non-repetition.[635] That State is also under an obligation to make full reparation for the injury caused, whether material or moral, by its wrongful act.[636] Restitution is maintained as the primary form reparation, but if restitution is unavailable,[637] compensation is payable for financially assessable loss.[638] Where injury results

629. Crawford, *supra* note 49, at 662.

630. Draft Articles, art. 21.

631. *See supra* notes 534-617.

632. *Information Warfare as International Coercion, supra* note 5.

633. Terry, *Responding to Attacks, supra* note 361, at 185.

634. Draft Articles, art. 29.

635. *Id.* art. 30.

636. *Id.* art. 31.

637. *Id.* art. 36.

638. *Id.* art. 37.

that cannot be made good by either restitution or compensation, the responsible State is obliged to give satisfaction for the injury caused,[639] such as a formal apology or an expression of regret.[640]

i.) Authorities/Organs of a State

The conduct of any State organ shall be considered an act of the State concerned provided that organ was acting in that capacity.[641] The organ may belong to the constituent, executive, legislative, judicial, or other power.[642] Conduct by entities exercising elements of governmental authority shall likewise be considered an act of that State.[643] The State shall remain liable even if the authorities or organs acted beyond their authority or contrary to the instructions given;[644] ultra vires not being a defense for State responsibility.[645] Thus, if, for instance, it was the Philippine Secretary of Defense who conducted or commanded the cyberattack against another State, that other State may attack the Philippines with the same intensity. The Philippines shall likewise be liable to make reparations.

ii.) Acting under the Instructions or Control of the State

According to Article 8 of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, the conduct of a person or group of persons shall be considered an act of the State under international law if the person or group of persons was in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.[646] According to the World Court in Nicaragua, for a State to be legally responsible, it would have to be proved that the State had effective control of the operations in the course of which the alleged violations were committed, which may be inferred from the fact that the leaders were selected by the State, and from other factors such as the organization, training, and equipping of the force, planning of operations, the choosing of targets, and the operational support provided.[647] To illustrate, the Philippines

639. *Id.* art. 38.

640. Crawford, *supra* note 49, at 667.

641. Draft Articles, art. 4.

642. *Id.* art. 4.

643. *Id.* art. 5.

644. *Id.* art. 9.

645. HARRIS, CASES AND MATERIALS, *supra* note 1, at 504.

646. Draft Articles, art. 8.

647. *Nicaragua*, 1986 I.C.J. at 62, ¶ 101 (emphasis supplied).

would be liable for sending a virus if it was the Defense Secretary of the Philippines who hired and taught the cyberattacker the weakest and intricate points of another State's critical information systems.

b) Indirectly: Aiding, Abetting, or Financing

Aid or assistance is relevant in attribution with respect to a State's participation in a breach committed by another State, but not if such aid or assistance is given to an individual within the territory of that State.[640] The World Court has however recognized that assistance or logistical support to individuals, although not constituting an armed attack, may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States.[649] This is because a State is obligated to refrain from organizing, instigating, assisting, or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts.[650]

The act of aiding, abetting, or financing forcible activities against other States[651] is contrary to the duty not to knowingly allow one's territory to be used for acts contrary to the rights of other States.[652] As international law strictly prohibits intervention by one State in the sovereign affairs of another State,[653] State support[654] of cyberterrorist activities constitutes a breach of this customary duty of non-intervention. For if a State aided or assisted in the carrying out of an attack from its territory, then State knowledge of such harmful activities is present, hence, a violation of the duty not to knowingly allow one's territory to injure other States.[655]

As a response, since such attack does not constitute an armed attack, the right of self-defense cannot be invoked against a State aiding or abetting such attack. States, however, should still be allowed to resort to counter measures[656] or to break diplomatic relations with countries sponsoring any

648. Draft Articles, art. 16.

649. *Id.*

650. G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N. Doc.A/8028 (1970).

651. *Id.*

652. *Corfu Channel*, 1949 I.C.J. at 4.

653. U.N. CHARTER, art. 2(7); Jackamo, *From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary Law of Non-Intervention*, 32 VAND. J. INT'L L. 929 at 953 (1992); *Nicaragua*, 1986 I.C.J. 103, at 108.

654. Ian Brownlie, *International Law and the Activities of Armed Bands*, 7 I.C.L.Q. 712, 734 (1958) [hereinafter Brownlie, *Armed Bands*].

655. DINSTEIN, *supra* note 508, at 236.

656. Draft Articles, art. 22.

terrorist actions, such as when Western European countries and the United States expelled Libyan diplomats suspected of engaging in terrorist activities.[657] Economic sanctions provide leverage against terrorism, although they are difficult to impose because they require widespread international cooperation. An example would be the United States' economic embargo against Iran and Libya in the 1980s and 1990s, as did the United Nations against Afghanistan in 1999.

2. During the Act

A State acknowledging and adopting the acts of an individual is directly liable for the acts committed by such individuals and may respond the same way as in responding to a State controlling or instructing such individuals. Thus, the attacked State may exercise the right of self-defense against a State acknowledging and adopting the cyberattack. Also, the attacked may require the latter to comply with the obligation breached,[658] to cease the wrongful act,[659] and to make full reparation for the injury caused.[660]

An initially private conduct becomes an act of the State only if, and to the extent, that the State acknowledges and adopts the conduct as its own.[661] According to Article 11 of the Draft Articles on the Responsibility of States for International Wrongful Acts:

> Conduct which is not attributable to a State under Articles 4, 5, 6, 7, 8, or 10 shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.

To expound, the acknowledgment and adoption must be cumulative, unequivocal, and unqualified.[662] Article 11 was meticulously crafted in order to prevent any attribution based on mere endorsement or ratification. This is evident from the Commentary of the International Law Commission as Article 11 is a codification of what various tribunals have done in the past, particularly in the Lighthouses Arbitration[663] and Diplomatic and Consular

657. To get the full account thereof, *see* J.P. WOOTEN, TERRORISM: U.S. POLICY OPTIONS (1988).

658. Draft Articles, art. 29.

659. *Id.* art. 30.

660. *Id.* art. 31.

661. *Id.* art. 11.

662. Commentaries to the Draft Articles, *supra* note 569.

663. 12 U.N.R.I.A.A. 155, 198 (1956).

Staff in Tehran Case,[664] where attribution of an act to a State was based on an acknowledgment and adoption of the conduct of the individual.[665]

In the Lighthouses Arbitration, Greece was held liable for the breach of contract committed by Crete because the former endorsed the breach by the latter, effectively continuing the breach of contract. In the Diplomatic and Consular Staff Case, the Court held Iran liable for the hostage taking of the U.S. embassy because the Ayatollah Khoumeini told the students that it was up to them to expand with all their might their attacks against the United States.[666] It was the seal of governmental approval to the acts involved and the decision to perpetuate them, which translated the continuing occupation of the embassy into acts of Iran, as can be gleaned from the following statements of the World Court:

> The seal of official government approval was finally set on this situation by a decree issued on 17 November 1979 by the Ayatollah Khoumeini. His decree began with the assertion that the American Embassy was a 'centre of espionage and conspiracy' and that 'those people who hatched plots against our Islamic movement in that place do not enjoy international diplomatic respect.' He went on expressly to declare that the premises of the Embassy and the hostages would remain as they were until the United States had handed over the former Shah for trial and returned his property to Iran...
>
> ...The approval given to these facts by the Ayatollah Khoumeini and other organs of the Iranian State, *and the decision to perpetuate them*, translated the continuing occupation of the Embassy and detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible....[667]

It is clear in both cases that the endorsements by Greece of the breach and Iran of the hostage-taking, were held sufficient for attribution because they effectively translated the continuing delict into an act of State.[668]

It must be noted that for Article 11 to apply, the endorsement of the State should translate a continuing act into an act of State. Conduct is not attributable to a State where the State merely acknowledges the factual situation or expresses verbal approval or support subsequent thereto.[669] Clearly, therefore, the endorsement should happen during the act, not thereafter.

664. US Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3.

665. Commentaries to the Draft Articles, *supra* note 569.

666. *Tehran Hostages*, 1980 I.C.J. 3, at ¶ 59.

667. *Id.* at ¶¶ 73-4.

668. Commentaries to the Draft Articles, *supra* note 569.

669. *Id.*

For instance, if an individual from the Philippines hacked the air traffic control system of another State resulting in a plane collision and the President of the Philippines subsequently proclaims the hacker as a "hero of a just world,"[670] the endorsement will not fall under Article 11, but in some other form of attribution, for example, harboring a cyberterrorist.

The author takes pains to point out that on one hand, a perusal of Article 11 would make it appear that the same has no application to a cyberattack. This is because Article 11 presupposes a "duration of time" during which the effects of the unlawful conduct are felt, in order that, first, the seal of governmental approval may be given, resulting in, second, the decision by the actual wrongdoer to perpetuate his illegal acts. Arguably therefore, Article 11 is irrelevant in a cyberattack, since the time interval between the execution of a rogue program and its effects being felt are nearly instantaneous (in most instances, the time needed for a virus/worm to install itself is a matter of mere seconds); hence, the requisite "time duration" may be deemed to be absent.

On the other hand, the author submits that Article 11's requisite "time duration" can nevertheless be present, as long as the objective phase of the cyberterrorist attack has not ended, e.g., as long as the effects of a cyberattack or a virus are, or may still be, felt. The author presents the following illustrative examples:

First, should a cyberterrorist transmit one virus carrying 2 waves of attacks, and the second wave is programmed to activate itself only after an appreciable period of time has lapsed after the first wave.

Second, a virus takes over the control system of an airplane, a train, or vessel at 9:00 a.m., but the vehicle crashes only at 9:30 a.m. Any time in between 9:00 a.m. and 9:30 a.m. constitutes the requisite "time duration" for an acknowledgment and adoption to occur.

Third, from the time the effects of a virus are first felt until the time an antidote, in the form of a countervailing software program, has been effectively discovered, e.g., in the case of "Melissa" or "I love you" (these viruses, before crashing the hard disk of the computer so infected, would e-mail themselves to all e-mail addresses found in the infected computer).

Article 11 does not also envision successive successful cyberattacks. For instance, if after the Filipino hacker has successfully attacked, and the President told the hacker to hack once more, and the hacker attacked again, Article 11 will not apply. The Philippines shall, however, be liable under Article 6 of the Draft Articles as to the second attack, since the element of

670. *See, e.g.*, Phillip C. Jessup International Law Moot Court Competition, Compromis de Arbitrage (2002), *available at* http://www.ilsa.org (last visited Feb. 1, 2002).

control or instructions by the State existed from the commencement of the second attack. To clarify, the Philippines shall be liable only for the second attack, but not for the first attack, since the subsequent act of the President is immaterial with respect to the consummated (the first) attack.

3. Post Facto - Harboring

As there exists an obligation for States not to permit their territory to be used as a haven for any attacks against military or civilian objects in another country,[671] all States are now obliged to cease any provision of sanctuary for international terrorists and to ensure that the territory under its control is not used for terrorist installations and camps.[672] Serious crimes of international concern create an obligation erga omnes for States to either surrender the terrorist found in their territory to a competent tribunal, or, to prosecute him.[673] Therefore, a State is under a strict duty of "vigilance"[674] in prosecuting a terrorist found within its territory, in order not to render moot or circumvent the international duty to suppress terrorism.

In ensuring that a cyberterrorist is brought to justice, the victim-State has three options when the cyberterrorist is found in another State. The victim-State may avail of extradition, if an appropriate extradition treaty has been entered into. However, absent an extradition treaty or the State refuses extradition or fails to perform its obligation of due diligence in searching for the fugitive, the victim-State may go to the Security Council for assistance. Recent developments in international law have also provided another remedy for States – irregular rendition. However, in availing of this latter remedy, the author submits that a State should confine the luring within strictest limitations to avoid any violation of the rights of the criminal and of the harboring State.

a) Extradition

Extradition is the international judicial rendition of fugitives charged with an extraditable offense and sought for trial, or already convicted and sought for punishment.[675] More specifically, it is the duty of a State on the territory of which an accused or convicted person has taken refuge, to deliver him up to another State which has requisitioned his return and is competent to judge

671. *See* Brownlie, *Armed Bands*, *supra* note 655, at 734 (1958); DINSTEIN, *supra* note 508, at 238.

672. S.C. Res. 1368, U.N. Doc.S/RES/1368 (2001); S.C. Res. 1373, U.N. Doc.S/RES/1373 (2001); S.C. Res. 748, U.N. SCOR, 47th Sess., U.N. Doc.S/23992 (1992).

673. Goodwin-Gill, *supra* note 622, at 206.

674. R. Agro, *Fourth Report on State Responsibility*, II I.L.C. Y.B. 71, 120 (1971).

675. WHITEMAN, *supra* note 537, at 727.

and punish him.[676] Through the use of extradition treaties, States may successfully request the return of terrorists from other States in order that such criminal may stand trial before its local courts.[677] It has been said:

> Extradition is a technical process that requires precision and cooperation between two sovereign systems, often different in fundamental legal theory and procedure. An extradition represents an attempt by nation-states, through diplomatic and legal means, to cooperate in rendering fugitive criminals to another. Of course, when nations cooperate in criminal matters, they give up some of their sovereignty. The extradition process is designed to accomplish this goal without seeming to diminish either party's sovereignty or to by pass or demean either's institutions or processes, or basic theories of criminal justice, including the traditional rights of the accused fugitive. This is no easy task, and it is not made any simpler by the fact that the terms of the extradition treaty have meaning only when applied to disparate legal concepts and processes. These, in turn, have meaning only within each country's given cultural, linguistic, and anthropological frame of reference.[678]

Many authors have asserted that the extradition doctrine has been rendered outdated because of the increase in international crimes, particularly, terrorism.[679] Like extradition, the laws governing computer crimes struggle to keep pace with rapid technological advancements that threaten to leave the law an archaic relic in the distant past.[680] This fact has important implications for extradition as the process requires double criminality.[681]

The rule of double criminality in extradition requires that an act shall not be extraditable unless it constitutes a crime according to the laws of both the requesting and the requested States.[682] Double criminality protects States' rights by promoting reciprocity and also safeguards an individual's rights by shielding him from unexpected and unwarranted arrest and imprisonment.[683] An exception to double criminality is when the requesting State merely asks

676. BASSIOUNI, INTERNATIONAL EXTRADITION, *supra* note 317, at 1 (1974); F. DE CARDAILLAC, DE L'EXTRADITION 3-4 (1875).

677. Laflin, *Kidnapped Terrorists: Bringing International Criminals to Justice through Irregular Rendition and Other Quasi-legal Options*, 26 J. LEGIS. 315 (2000) [Laflin, *Kidnapped Terrorists*].

678. BLAKESLEY, TERRORISM, *supra* note 124, at 172.

679. Soma, *Transnational Extradition*, *supra* note 331, at 317.

680. *Id.*

681. Emami v. U.S. District Court, 834 F.2d 1444, 1448 (9th Circ. 1987).

682. I.A. SHEARER, EXTRADITION IN INTERNATIONAL LAW 137 (1971) (citing Benz, Das Prinzip der identischen Norm im internationalem Austlieferungsrecht [1941]).

683. BASSIOUNI, INTERNATIONAL EXTRADITION, *supra* note 317, at 314.

for the return of one of its own nationals who has committed a crime punishable in the requesting State.[684]

Since extradition treaties specify which offenses will be extraditable through a listing of extraditable offenses contained in the treaty itself or in an attached appendix, extradition of cyberterrorists shall encounter numerous problems. As explained earlier, present domestic laws criminalizing cyberattacks are far from uniform, and provide for varying degrees of enforcement. A more problematic situation is where the State of refuge (or the requested State) has no law penalizing the crime, and the perpetrator is not a national of the requesting State.

In the Philippine context, the E-Commerce Act only penalizes hacking; cyberterrorism is still sought to be criminalized through House Bill 3802. While some countries, such as the United States,[685] are willing to liberalize treaty interpretation of double criminality, other States are still unwilling to bend over backward as to a strict interpretation of the rule.[686] Therefore, there is no consistent State practice as to how the principle of double criminality should be applied. As such, the Philippines is not bound to follow either interpretation of the rule. However, since the Philippines has shown that its practice is to penalize crimes even those which are universal, it is recommended that the Philippines should pass a law so as to be consistent with its own practice. To reiterate, the proposed definition of cyberterrorism under House Bill 3802 must be amended in order to conform to how the greater majority of interested States define it.

b) Invoke the Aid of the Security Council

If a State refuses to cooperate in bringing a terrorist to justice, the Security Council may be requested to order the harboring State to extradite the terrorist found within its territory.[687] The Council is charged under Article 24 with the primary responsibility for the maintenance of international peace and security and has a mandate from all Member States to act on their behalf in this regard.[688] By Article 25, all Members agree to accept and carry out

684. Soma, *Transnational Extradition*, *supra* note 331, at 324; BLAKESLEY, TERRORISM, *supra* note 124, at 237. *See, e.g.*, Extradition Treaty, May 4, 1978, U.S.-Mex. Art. 1, ¶ 2, T.I.A.S. No. 9656, at 5061-62.

685. U.S. v. Deaton, 448 F. Supp. 532 (N.D. Ohio, 1978).

686. Jonathan Hafen, *International Extradition: Issues Arising Under the Dual Criminality Requirement*, 1992 B.Y.U. L. REV. 191 (1992).

687. S.C. Res. 731, U.N. SCOR, 47th Sess., U.N. Doc.S/RES/731 (1992).

688. Case Concerning the Interpretation and Application of the Montreal Convention Arising of the Aerial Incident at Lockerbie (Libya v. UK), 1992 I.C.J. 3 (Provisional Measures) (Weeramantry, J., dissenting).

the Council's decisions.[689] Chapter VII gives the Council special powers when it determines the existence of any threat to the peace, breach of the peace, or act of aggression.[690] When the Council determines a breach of the peace, as what happened in the Haiti Incident,[691] it may call Member States to impose measures commensurate with the specific circumstances as may be necessary, including the conduct of a maritime embargo or sending troops to restore peace.[692]

In its Resolution 748, the Security Council required Libya to return the alleged offenders and imposed sanctions against it for not doing so.[693] Likewise, the Council imposed sanctions on Sudan for failure to extradite terrorists suspected of attempting to assassinate the Egyptian President in 1996.[694] Parenthetically, the Security Council may exercise its powers under Chapter VII of the U.N. Charter notwithstanding a case has been filed before the World Court.[695]

The author emphasizes that, in the case of harboring a terrorist, a suit for restitution or compensation before the World Court is not precluded. However, it must be noted that the harboring State will not, most likely, be ordered to compensate the victim-State for the acts done by the perpetrator. Nevertheless, the harboring State will be held liable for failing to comply with its duty to exercise due diligence in apprehending the fugitive, which includes payment of damages. In the Janes case,[696] Mexico was ordered to pay damages to the United States because of the former's unreasonable delay and failure in arresting a Mexican national who killed an American citizen in Mexico. All the more should this remedy apply when what is involved is not a mere domestic crime, but one which triggers universal jurisdiction.

c) Luring

If no extradition treaty exists and the State breaches and refuses to perform its duty of due diligence in prosecuting or surrendering a cyberterrorist, and the Security Council fails to act upon the matter, is the victim State left without a remedy? In such case, it has been said that irregular rendition to acquire jurisdiction over a criminal may be appropriate, provided, the

689. U.N. CHARTER, art. 25; HARRIS, CASES AND MATERIALS, *supra* note 1, at 1043.

690. U.N. CHARTER, Chapter VII.

691. S.C. Res. 841 & 873, *reprinted in* RESOLUTIONS AND DECISIONS 119, 125 (1993).

692. HARRIS, CASES AND MATERIALS, *supra* note 1, at 944.

693. S.C. Res. 748, U.N. SCOR, 47th Sess., U.N. Doc.S/23992 (1992).

694. S.C. Res. 1044, 1054 and 1070, U.N. SCOR, 51st Sess., U.N. Doc.S/RES/1044, U.N. Doc.S/RES/1054, U.N. Doc.S/RES/1070 (1996).

695. *Lockerbie*, 1992 I.C.J. 3 (Judge Weeramantry, Dissenting); HARRIS, CASES AND MATERIALS, *supra* note 1, at 1044.

696. U.S. v. Mexico, 4 R.I.A.A. 82 (1925).

prosecuting State uses only such means as are necessary to apprehend the foreign fugitive.[697] It must be borne in mind that resort to irregular rendition must be exercised with due respect to the territorial integrity of the harboring State and to the established rights of the criminal.

Irregular rendition is the process of capturing an international fugitive from justice outside the existence or the parameters of an extradition treaty.[698] Since the mid-1980s, several high-profile international terrorists have been brought to trial through irregular rendition. The author however asserts that not all irregular renditions are valid in light of international human rights law.

As a rule of customary law, the International Covenant on Civil and Political Rights provides for the right to liberty and security of person, except on such grounds and in accordance with such procedure as established by law.[699] The same right is embodied in various international human rights conventions.[700]

Indeed, there is a close relationship between terrorist acts and the enjoyment of human rights and fundamental freedoms.[701] This relationship can be seen indirectly when a State's response to terrorism leads to the adoption of policies and practices that exceed the bounds of what is permissible under international law, and results in human rights violations, such as arbitrary detentions, torture and other acts that violate the rights of the terrorist, himself.[702]

The author concedes that it has been posited that by virtue of the principle of male captus, bene detentus[703] a person being tried for an offense may not oppose his trial by reason of the illegality of his arrest.[704] In many cases, States have been allowed to resort to forcible abduction in order to acquire jurisdiction over a criminal found within the territory of another

697. Laflin, *Kidnapped Terrorists*, *supra* note 678, at 315.

698. *Id.*

699. ICCPR, art. 9. *See* Report of the Working Group on Arbitrary Detention, U.N. ESCOR, Hum. Rts. Comm., 50th Sess., Agenda Item 10, at 39-40, U.N. E/CN.4/1994/27 (1993).

700. UDHR, arts. 3 & 9; ECHR, art. 5; African Charter, art. 6; American Declaration, arts. 1 & 25.

701. Koufa, *supra* note 52, at 213.

702. *See id.*

703. *Compare* U.S. v. Yunis, 859 F.2d. 953 (D.C. Circ. 1988) *and* Paul Koring, *Kirds Enrages Rebel Chief Snatched*, GLOBE & MAIL, Feb. 17, 1990. *With* Stocke v. Federal Republic of Germany, 95 I.L.R. 328, 347-8 (1989).

704. M. CHERIF BASSIOUNI, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE 190 (1987).

State.[705] However, sufficient State practice[706] has opposed this principle laid down in the Eichmann[707] case and the Alvarez Machain[708] case. The author asserts that forcible abduction violates the territorial integrity of another State and the criminal's right to security of person;[709] perforce, kidnapping is prohibited under International law.[710] To rule out the invocation of a violation of the right to security of person as a ground to invalidate the arrest is to leave international human rights law without any grinding teeth and within the realm of hortatory law.

Interestingly, the prohibition against the exercise of jurisdiction on the basis of a human rights violation due to forcible abduction applies when the conduct of the government in acquiring custody amounts to grossly cruel and unusual barbarities, or to acts that shock the conscience, as held in the Toscanino Case.[711] In Toscanino, the U.S. agents forcibly took the criminal from Uruguay and brought him to Brazil where he was tortured. However, Toscanino still involved physical coercion that should invalidate the acquisition of jurisdiction by the abducting State, since a criminal should not be treated as having waived his right to physical integrity.[712]

Is the victim State, then, left without a remedy?

705. *See* Attorney-General of the Government of Israel v. Adolf Eichmann [Eichmann Case], 36 I.L.R. 5 (1968); Ker v. Illinois, 119 U.S. 436 (1886); Frisbie v. Collins, 342 U.S. 519 (1952); Levinge v. Director of Custodial Services, 9 N.S.W.L.R. 546 (New S. Wales (Austl.) C.A. 1987).

706. Regina v. Horseferry Rd. Magis Ct. (*Exparte* Bennett), [1994] 1 App. Cas. 42 (Eng. H.L. 1993); State v. Ebrahim [1991] 2 S.A.L.R. 552 (S. Afr. App. Div.), *summarized and translated in* 31 I.L.M. 888(1992).

707. Eichmann case. Eichmann was kidnapped by U.S. authorities in Argentina. His kidnapping was not declared illegal under international law.

708. United States v. Alvarez-Machain, 504 U.S. 655 (1992). In this case, Alvarez-Machain was abducted by U.S. authorities with the connivance of Mexican police. The U.S. Court stated that the illegality of an arrest does not affect the jurisdiction of a court.

709. Paul Michell, *English-Speaking Justice: Evolving Responses to Transnational Forcible Abduction After Alvarez-Machain*, 29 CORNELL INT'L L.J. 383, 410-36 (1996).

710. Michael Scharf, *The Tools for Enforcing International Criminal Justice in the New Millenium: Lessons from the Yugoslavia Tribunal*, 49 DePaul L. Rev. 925, 964 (2000) [hereinafter Scharf, *The Tools*].

711. U.S. v. Toscanino, 500 F.2d. 267 (2nd Circ. 1974), *reh'g denied*, 504 F.2d 1380 (2nd Cir. 1974), *on remand*, 398 F. Supp. 916.

712. Susan Coutin, *Ethnographies of Violence: Law, Dissidence and the State*, 29 L. & SOC'Y REV. 517, 529-37 (1995).

In the case of Liangsiprasert v. U.S.,[713] it has been stated that police forces should be accorded a certain leeway to combat sophisticated international criminal activity through the use of ruses and tricks. As evidenced by extensive State practice and opinio juris, one method of irregular rendition has come to be accepted as the most reasonable and proportional, in fact legal, irregular rendition – luring.[714]

Luring is the mere employment of trickery,[715] such as a promise of immunity or any concession,[716] in order to induce an international fugitive to surrender on the belief that he will not face prosecution.[717] Unlike in forcible abductions, no physical or moral compulsion[718] is used in luring. As the term "luring" implies, a State cannot send its agents into another State to abduct an individual for trial, as the weight of authority holds that such would be an irreprehensible breach of the territorial sovereignty of the State where the fugitive is located and a violation of the rights of the fugitive as well.[719]

As distinguished from kidnapping, luring violates neither the human rights of the criminal, nor a State's territorial sovereignty.[720] Luring eliminates the potential offense of violating territorial sovereignty because no actual intrusion into another State's territory occurs. Moe importantly, luring does not violate the right against arbitrary detention (or the corollary right to liberty) of the criminal because no coercion is involved as no degree of duress is exercised over the criminal.[721] If at all, the offer is one that the criminal can still refuse.[722]

713. 1 App. Cas. 225 (1991).

714. Prosecutor v. Slavko Dokmanovic, Decision on the Motion for Release by the Accused Slavko Dokmanovic, No. IT-95-13a-PT, T., Ch. II, ¶¶16-18 (Oct. 22, 1997).

715. Paul Kurds, *Kurds Enrage as Rebel Chief Snatched*, GLOBE & MAIL, Feb. 17, 1999, at A1.

716. Stocke v. Germany. 13 EUR. H.R. REP. 834 (1991).

717. U.S. v. Yunis, 859 F. 2d. 953 (D.C. Circ. 1988).

718. *See* Schmidt I, (1995) 1 App. Cas. At 359; Colunje (Pan v. U.S.), (1933) 6 R.I.A.A. 342 (U.S.-Pan. Gen. Claims Commission).

719. Marchand, *Abductions Effected Outside Naitonal Territory*, 7 J. INT'L COMM'N JURISTS 243 (1966); O'Higgins, *Unlawful Seizure and Irregular Extradition*, 36 BRIT. Y.B. INT'L L. 279 (1960); Selleck, *Jurisdiction after International Kidnapping: A Comparative Study*, 8 B.C. INT'L & COMP. L. REV. 237 (1985).

720. *Ex parte* Brown, 28 F. 653 (N.D.N.Y. 1886); *In Re* Hartnett, 1 O.R. 2d 206 (Ont. (Can.) H.C.J. 1973); Colunje (Pan. V. U.S.), [1933] 6 R.I.A.A. 342 (U.S.-Pan. Gen. Claims Comm'n.).

721. U.S. v. Wilson, 732 F.2d 404 (5th Circ. 1984).

722. *Schmidt I*, 1 [1995] App. Cas. at 358.

Luring, however, must be distinguished from moral compulsion.[723] Luring does not contemplate a situation where the prosecuting State holds the family of the fugitive in hostage, in order to force the fugitive to surrender by delivering himself to the authorities, rather than allowing his family to be assaulted.

In the International Criminal Tribunal for the Former Yugoslavia (ICTY) case of Prosecutor v. Dokmanovic,[724] a member of the Office of the Prosecutor of the Yugoslavia Tribunal met with Slavko Dokmanovic in Serbia to lure the latter to Croatia, where he was subsequently arrested. Dokmanovic was, at the time of his arrest, charged with crimes against humanity and went into hiding in Serbia. Shortly after Dokmanovic was surrendered to the Yugoslavia Tribunal, he filed, through counsel, a Motion for Release, arguing that the manner of his arrest was illegal. However, the tribunal categorically rejected the argument, stating that the means used to accomplish the arrest neither violated principles of international law nor the sovereignty of Serbia;[725] in effect, declaring that luring is permissible in such circumstances.

Although the author agrees with the principle of luring as a permissible means to pursue a criminal jure gentium, States availing of this remedy should not exceed the threshold of what is reasonable to apprehend the fugitive. For instance, in the Dokmanovic case, the agent of the Office of the ICTY Prosecutor actually physically entered the territory of Serbia without its knowledge. The more prudent approach is that a State resorting to luring should not physically enter another State's territory without the latter's consent; instead, the prosecuting State should limit the luring through communications over the phone, radio or e-mail correspondence.

Neither should moral compulsion be employed such as holding the family of the criminal in captive, or fraudulently asserting that a family member is seriously under illness[726] because in such a case the criminal is left without a choice but to forcibly succumb to the desire of the prosecuting State in bringing him to justice.

The author reiterates that luring may only be exercised within these strict parameters: (1) the crime involved is a serious international crime, such as terrorism; (2) there is no extradition treaty, or in its absence, the harboring State refuses to prosecute and the Security Council fails to act upon the matter; (3) no physical or moral compulsion is involved.

723. *See id.* at 359; Colunje (Pan v. U.S.), (1933) 6 R.I.A.A. 342 (U.S.-Pan. Gen. Claims Commission).

724. *Dokmanovic*, No. IT-95-13a-PT, T. Ch. II.

725. Scharf, *The Tools*, *supra* note 711.

726. *See* PARAS, PHILIPPINE CONFLICT LAWS 34 (1996).

The rules articulated in this Chapter are presented in a matrix below.

RULES ON COUNTERING THE UNCONVENTIONAL

Cyberattack/ Activity	*Effects*	*Motive*	*Offender*	*Degree of Participation*	*Remedy/ Response*
Activism	Normal use of the Internet	None	Individual/s	By himself/ themselves	No responsibility/ liability
Hactivism	Intrusion into computer system	Political - usually proclaimed	Individual/s	By himself/ themselves	Domestic Prosecution
Cyberterrorism	1. Violence; , or 2. Serious Harm to Non-combatants	Political - which is *either:* 1. Proclaimed; or 2. If Not Proclaimed, *can be presumed* from: *a. The Actor:* being a known terrorist or a member in a known terrorist organization; and *b. The Act* i. Target: Critical Infrastructure ii. Effect: Violence *or* Serious Harm to Non-combatants (such effects get the attention of those in authority to heed a political grievance)	Individual/s	By himself/ themselves	Universal Jurisdiction
		With State Participation - amounts to: *Cyber-Use of Force*	Directly by State Authorities/ Organs Acting under the instructions or control of the State	a. Self-defense if cyberattack amounts to armed attack b. Countermeasures c. Sue before the International Court of Justice (ICJ)
			Aiding, Abetting, or Financing	a. Countermeasures b. ICJ
			Acknowledgment and Adoption	a. Self-defense b. Countermeasures c. Sue before the International Court of Justice (ICJ)
				Harboring	a. Go to Security Council b. Extradition c. Luring

VII. CONCLUSION AND RECOMMENDATIONS

With cyberattacks emerging as the new form of attacks, present international rules governing responses to such attacks call for a proper delineation of the responses to varying degrees of cyberattacks, as elucidated in the preceding Chapter. A proper understanding of these rules informs the attacked State as to what steps, and the limitations of those steps, it may lawfully take in countering the unconventional. It would not be amiss to point out that the rules on countering the unconventional require a careful consideration of whether such attacks were carried by individuals or caused by States and in case of the latter, whether State responsibility is engaged.

In responding, the attacked State must initially determine whether an individual attack is mere activism, or hacktivism, or cyberterrorism, since these different kinds of cyberattacks differ in terms of prosecution and jurisdiction. In case of a State-sponsored cyberattack, the victim-State must ascertain if an attack amounts to an armed attack attributable to a State in order to counter-attack in the name of self-defense. Although present international hard law (traditional sources of international law, mainly treaty and customary international law) seem to, a certain extent, encompass some of the aspects of these cyberattacks, they were adopted largely to address conventional attacks. Thus, the inadequacy of present rules shall be the subject of the author's conclusions and recommendations.

A. Attacks by Individuals

The response to a cyberattack committed by an individual, without any State sponsorship, is prosecution. Any State attacked by an individual through cyber-means must evaluate such attack in order to determine if such individual is prosecutable or not. As discussed, three categories of cyberattacks exist namely activism, hacktivism, and cyberterrorism.

Putting the last Chapter in a nutshell, activism cannot be criminalized nor prosecuted by a State because such activity merely springs from the fundamental right to expression, unless the State has restricted such right for reasons of national security, or protection of public order, or health or morals. In contrast, when the activity is intrusive, and tainted with a political purpose, but without causing violence or harm to civilians, this kind of cyberattack is subject to prosecution under municipal law under the general

crime of hacking. If the hacking was done by a Filipino, whether here or abroad, and the effects of the crime were felt here, he will be subject to prosecution under the E-Commerce law. However, a problem arises when the effects of the crime are felt in many States, and all these States claim jurisdiction over the person. The author concludes that all these States, by virtue of the objective territoriality principle, and the national State, by virtue of the nationality theory, have basis to claim jurisdiction. At present, international law does not resolve this issue. The only treaty dealing with cybercrimes, the European Convention on Cybercrimes, which has not yet entered into force, does not resolve these conflicting claims of jurisdiction. Article 22 of said Convention states:

> Jurisdiction
>
> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2-11 of this Convention, when the offence is committed :
>
> a. in its territory; or
>
> b. on board a ship flying the flag of that Party; or
>
> c. on board an aircraft registered under the laws of that Party; or
>
> d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
>
> 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof.
>
> 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.
>
> 4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.
>
> 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

The author recommends that State priority in jurisdiction must be established, applying, by analogy, certain parameters of extradition law and the principle of forum non conveniens in private international law. The State where the crime was performed should have primary jurisdiction, only if the offender is physically present when the offense occurred, since this will ease and facilitate the prosecution of the offender. Second, the State where substantial effects are felt should have jurisdiction, if the State with primary jurisdiction refuses or fails to prosecute, but only after a demand to prosecute has been made by the former to the latter. In case many States claim that substantial effects were felt within their territory, the State having the largest damage should have jurisdiction. In case the damage is substantial but not capable of pecuniary estimation or the States suffered equivalent substantial effects, the State that first takes steps to prosecute the perpetrator, in accordance with its domestic law, shall have jurisdiction. These rules of jurisdiction shall, however, not preclude the national State from requesting for extradition from the prosecuting State. These rules may be contained in a new treaty or inserted in the European Convention which will read as follows:

> Jurisdiction
>
> 1.) The State where the offender performed the crime shall have primary jurisdiction in case the offender is physically present in the territory of that State.
>
> 2.) If the State with primary jurisdiction fails or refuses to prosecute, the State where substantial effects are felt shall have jurisdiction but only after a demand to prosecute has been done by the latter to the former.
>
> In case, many States will claim that substantial effects were felt within their territory, the State having the largest damage shall have jurisdiction. In case the damage is substantial but not capable of pecuniary estimation or the States had felt same substantial effects, the State first taking step in prosecuting the perpetrator, in accordance with its domestic law, shall have jurisdiction.
>
> 3.) These rules do not preclude the national state from requesting extradition from the prosecuting state.

With respect to cyberterrorism, an attack to be characterized as such must: (a) be against a critical infrastructure; (b) have a political motive; and (c) cause violence or severe economic hardship to civilians and non-combatants. Any other civil disobedience must be limited to either activism or hacktivism.

Unlike in hacktivism, all States, by virtue of the universality principle, have jurisdiction over the crime committed by a cyberterrorist regardless of whether the effects of the crime are felt within the territory of such States. Yet, in cases of cyberterrorism, the State where the offender is physically present when the offense occurs shall still have primary jurisdiction over the prosecution of the perpetrator. However, as previously discussed, the Philippines adheres to enacting a law that will punish such crime despite its universal character. In this regard, the definition of "cyberterrorism" in House Bill 3028 is the same as the crime of "hacking" defined by the E-

Commerce Law,[727] thus overlooking the disparity in gravity of each offense by treating them synonymously.

To reiterate, House Bill 3028 defines cyberterrorism as:

> [U]nauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents.[728]

The author recommends an amendment to this bill, such that it reads consistently with international legal norms:

> Cyberterrorism is a politically motivated attack, through the use of computers and against computers controlling critical infrastructure, resulting in violence or serious economic hardship to civilians or non-combatants, generating a state of terror in the minds of the general public.
>
> The phrase 'Critical infrastructure,' when used in this Act, refers to those national systems so vital to the State that their incapacity or destruction would have a debilitating impact on the defense or economic security of the State which includes, but is not limited to: telecommunications, transportation, electric power systems, banking and finance, water supply systems, gas and oil storage and transportation, emergency services (medical, police, fire and rescue), and other infrastructure, closely intertwined with civilian life and relating to the continuity of government.

Of course, this is without prejudice to, assuming the availability of resources, the establishment of a Commission on Critical Infrastructure Protection, which will focus, not on the post-crime activities such as prosecution, but the deterrence of cybercrime and the protection of Philippine critical infrastructure, similar to the commissions/committees established in the U.S., Japan, and European Community.

727. R.A. 8792, § 33. Under R.A. 8792, hacking or cracking is defined as the "unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of elctronic data messages or electronic document."

728. H.B. 3802, Section 3(i), 12th Congress, First Regular Sess. (2001).

B. Attacks with State Participation

Two vital points have been raised by the author with respect to the exercise of the right of self-defense. First, a cyberattack constitutes an armed attack when it results in massive destruction. As such, it triggers the right of self-defense. Second, when sufficient evidence exists that a State plans to use information stolen after intrusion into computer systems from which it gained military (tactical) advantage, such instance triggers anticipatory self-defense. However, in the latter case, the burden to prove the imminence of the attack lies with the counter-attacking State.

The wording of Article 51 of the Charter, however, results in different interpretations by scholars. The present text, in pertinent part, reads:

> 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 measures necessary to maintain international peace and security.

As previously explained, customary international law has shown that anticipatory self-defense is permissible; in the least, it is not prohibited. Although the author has sufficiently proved that both article 51 and anticipatory self-defense should apply in two instances of cyberattacks, a declaration to this effect would be advisable. In a rapidly changing world, General Assembly Resolutions have been regarded as the most acceptable method, albeit restricted by the rule of unanimity or quasi-unanimity, of adapting the principles of the U.N. Charter and the rules of customary international law to the changing times with an efficiency which even its most optimistic founders did not anticipate.[729] The author therefore recommends the adoption of a General Assembly Resolution Defining the Right of Self-Defense in the Cyber Age. This Resolution will read as follows:

TEXT OF PROPOSED GENERAL ASSEMBLY RESOLUTION

Declaration on the Definition of the Right of Self-Defense in the Cyber Age

The General Assembly,

Considering that after General Assembly Resolution 53/70 was adopted, States have taken steps to combat cyber attacks against critical infrastructure,

Bearing in mind that attacks against critical infrastructure threaten domestic stability and international peace and order,

In view of the fact that a cyberattack against critical infrastructure may result in large and substantial effects,

729. SOHN, THE PRESENT STATE OF INTERNATIONAL LAW AND OTHER ESSAYS 39 (Bos ed., 1973).

Having regard to the inevitable use of the right of self-defense under Article 51 of the UN Charter against these kinds of attacks,

Guided by the purposes and principles of the Charter of the United Nations,

Solemnly declares,

Article 1. States are allowed to invoke article 51 of the Charter, referring to the right of self-defense, against a State attacking their critical infrastructure systems as herein provided.

Article 2. An attack, through the use of any computer system, against a computer system controlling *critical infrastructure* which results in massive destruction triggers an immediate exercise of the right of self-defense.

Article 3. Notwithstanding the previous article, a State that has been subject to an intrusive attack against computer systems containing information relating to national security, or civilian safety or welfare may invoke the right of self-defense to prevent an imminent attack, by the same State, against its critical infrastructure systems. However, this does not preclude the State subject of the self-defense measure to question the imminence of its alleged attack. Nothing in this article limits the applicable rules found in the Laws of Armed Conflict.

Article 4. Any exercise of the right of self-defense under this Resolution shall always comply with what is reasonable necessary and proportional to counter the attack posed.

This proposal is in line with the practice of the General Assembly to adopt a Resolution to put to rest any doubt as to the application of the provisions of the U.N. Charter in a changing global environment. The adoption of General Assembly Resolution 3314 defining the word 'aggression,' and Resolution 2625 laying down the Principles of Friendly Relations, have both proved the beneficial use of Resolutions to clarify the precise extent and scope of the meaning of the Charter.

Clearly, the dawn of the Cyber Age has transformed the way transnational conflict may be conducted. The author hopes that the clarification of jurisdictional issues over cybercrimes, the precise definition of cyberterrorism, and the conclusion that a cyberattack may qualify as an armed attack, shall prove helpful in responding to these new forms of attacks. Only by making domestic legislation congruent and consistent with international law norms can prevention, deterrence, and perhaps elimination, of aggression be possible. Moreover, only by redefining an inherent right limited by a general treaty provision can uphold the meaning of sovereignty and territorial integrity in this Age of Information.

The elimination of uncertainty in the application of accepted principles of international law may indeed remain elusive so long as technology continuously advances at a pace far more rapid than the law develops. While

conventional attacks may still be, in large part, par for the course, it is undeniable that the reduced risks of detection of and harm to cybercriminals make cyberattacks more desirable to them. Fortunately, any lag between technology and the law can be reduced by constantly instituting methods of reforms to reflect practical necessity and reasonableness. And as individuals and States continue to explore technology to better equip themselves in conflicts, the purposes of the U.N. Charter may only be achieved by delineating rules on countering the unconventional.