The John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 2 *Journal of Computer & Information Law - Winter 2004*

Article 2

Winter 2004

Defining Cyberterrorism, 22 J. Marshall J. Computer & Info. L. 397 (2004)

Mohammad Iqbal

DEFINING CYBERTERRORISM

MOHAMMAD IQBAL†

I. INTRODUCTION

One of the areas of concern in the war on terrorism is cyberterrorism – the terrorism originating from the cyber world. Cyberterrorism has been defined as 'hacking' with a body count.[1] This is one of many definitions of cyberterrorism that exist. There is a lot of misinterpretation in the definitions.[2] There are no reported instances of cyberterrorism, and therefore, it is objectively impossible to assess the risk of an unrealized act of cyberterrorism. However, commentators have invented scenarios wherein a cyberterrorist attack can possibly take many forms involving mass disruption and/or mass destruction. For example,

> a cyberterrorist might hack into computer systems and disrupt domestic banking, the stock exchanges and international financial transactions, leading to a loss of confidence in the economy. Or, she might break into an air traffic control system and manipulate it, causing planes to crash or collide. Or, a terrorist could hack into a pharmaceutical company's computers, changing the formula of some essential medication and causing thousands to die. Or, a terrorist could break into a utility company's computers, changing pressure in gas lines, tinkering with valves and causing a suburb to detonate and burn.[3]

The scenarios seem surreal and some experts are skeptical about manifestation of such events. According to one expert, there is no such

† Attorney at Law, Elgin, Illinois; LLM Student, The John Marshall Law School, Chicago, Illinois. The author is indebted to Professor Todd Fleming at The John Marshall Law School, for his encouragement to write this article.

1. Chris Ames, Air Force News News Service, *Terror Can Be Just a Computer Away,* ¶ 1, <http://web.archive.org/web/19990202201520/www.af.mil/news/Feb1998/n19980206_980156.html> (Feb.6, 1998) (quoting Barry Collin, "he is the one who actually coined the word Cyber Terrorism").

2. Serge Krasavin, SANS (System Administration, Networking, and Security) Institute, *What is Cyber-terrorism,* <http://www.sans.org/rr/infowar/cyberterrorism.php> (accessed May 19, 2003) (also available at <http://www.crime-research.org/analytics/Krasavin>).

3. Marc D. Goodman and Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* 2002 UCLA J.L. & Tech. 3, §8 Cyberterrorism.

thing as cyberterrorism.[4] However, a survey of 725 cities conducted by the National League of Cities shows that Cyberterrorism ranks with biological and chemical weapons atop officials' list of fears.[5] The fear may be unreasonable, and the conclusion that a new form of terrorism originating from cyber world is on the rise premature. Because of the fear that the threat is out there, the U.S. government has appointed a cyber security czar, and legislators are considering passing laws concerning Cyberterrorism.

So far, no cyber attack has led to violence or injury to a person.[6] It is further recognized that the terrorists have not transitioned to using cyberspace as a weapon, and that cyberterrorism remains as yet an unrealized phenomenon. Nonetheless, there is an anticipation that cyberspace will become an essential terrorist tool.[7] Some consider Cyberterrorism a sizable niche,[8] while skeptics reject cyberterrorism as a mere myth.[9]

Whether cyberterrorism is a vehicle of mass disruption not distinguished from hacking, a vehicle of mass destruction, an "electronic Pearl Harbor" or a "digital Armageddon" ranking with biological and chemical weapons, or just a harassment tool is a widely debated issue.

Despite the numerous articles published on cyberterrorism, there is no single definition that prevails over others. Nonetheless, cyberterrorism is considered a serious cybercrime. A cybercrime is a type of crime that is different from other crimes that use traditional media. In order to combat the crime of cyberterrorism, it is essential that the elements of crime must be fair, clear, and definitive.

This article explores definitions of the term "cyberterrorism" in light of available literature and recent legislation in an attempt to distinguish cyberterrorism from other cyber activities and crimes.

A. CYBERSPACE

The word with prefix 'cyber-', or 'cyber', means an online activity. In

---

4. Joshua Green, Washington Monthly, *The Myth of Cyberterrorism - There Are Many Ways Terrorists Can Kill You - Computers Aren't One of Them,* ¶¶ 6, 7 <http://www.washingtonmonthly.com/features/2001/0211.green.html> (accessed May 14, 2003).

5. *Id.* at ¶ 2.

6. *Id.* at ¶ 6.

7. Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument For Anticipating Cyber-attacks*, 2002 J.L. Tech. & Pol. 1, ¶ 2.

8. Ronald Weikers and Kevin Cronin, *Cyber-terrorism Can Help Grow Your Firm – If you represent corporations, there's potential in this niche*, Law Technology News, 39 (March 2003).

9. Green, *supra* n. 4, at § Ankle Biters.

other words, a modem or networking must be involved.[10] Besides being a prefix, it is also a verb, not a noun. It is an activity unique to the Information or Knowledge Age.[11]

Cyberspace is defined as a bio-electronic ecosystem that exists anywhere phones, coaxial cables, optic lines, or electromagnetic waves are available.[12] Internet, virtual world, and cyberspace are synonymous. The cyberspace or "Internet is a worldwide network of computers that enable various individuals and organizations to share information."[13] The Internet is a network of not only computers, but also of networks. The extent of its vastness is unknown. About 72 million individuals log on to it every day, and its use is growing, tripling in size every year.[14] No one owns cyberspace or operates it with any central authority. "Politically, it makes governments obsolete."[15] As such, the Internet is a "unique and wholly new medium of worldwide human communication."[16] It allows computer users to access millions of Web sites and Web pages. A Web page is a computer data file that includes names, words, messages, pictures, sounds, and links to other information. "The World Wide Web is a publishing forum consisting of millions of individual Web sites that contain a wide variety of contents."[17] Web surfing and e-mail are Internet or cyberspace applications.[18]

In recent years, businesses have begun to use the Internet to provide information and products to consumers and other businesses.[19] The exponential growth in use of the Internet has vastly expanded the means of communication worldwide. Cyberspace enables people to share ideas over great distances and engage in the creation of an entirely new, diverse, and chaotic democracy free from geographic and physical constraints. While the demonic potential of cyberspace is well recognized,[20] "less known is the fact that one can reach audiences of thousands or even

10. Tom O'Connor, *Cybercrime: The Internet As Crime Scene* ¶ 3, <http://faculty.ncwc.edu/toconnor/315/315lect12.htm> (accessed May 19, 2003).

11. *Id.* Further, Professor O'Connor explains that when you cyber, there is always action, motivation, movement, and interaction. "It is impossible to just *be* cyber. There is no steady state of being cyber. To cyber means that you are exchanging information, and you are constantly using technology. You are doing both at the same time – use of technology is to cyber." *Id.*

12. O'Connor, *supra* n.10 (quoting Esther Dyson, et al, *Cyberspace and American Dream*, <www.eff.org> (1994)).

13. *Panavision International, L.P. v. Toeppen*, 141 F.3d 1316, 1318 (9th Cir. 1998).

14. O'Connor, *supra* n. 10, at ¶ 5.

15. *Id.*

16. *ACLU v. Reno*, 929 F. Supp. 824, 844 (E.D. Pa. 1996), aff'd 521 U.S. 844 (1997).

17. *Yahoo, Inc. v. La Ligue Contre Racisme at Law Antisemitisme*, 169 F. Supp. 2d 1181, 1183 (2001).

18. *Panavision*, 141 F.3d at 1320.

19. *Id.* at 1321.

20. *ACLU*, 929 F. Supp. at 835.

millions in ways that conceal his or her identity."[21]

B. CYBERCRIME

A cyber-activity is very different from the use of computers for a traditional activity. It is like the difference between those who use computers for all they can be and those who use computers as a tool like a typewriter.[22] Cybercrime is substantially different from computer crime. Some argue that cyber theft is substantially different from other thefts using traditional media.[23] Cyberterrorism is clearly different from terrorism.[24]

Not every computer-related crime is a cyber-crime. The use of computers as incidental to another offense is not cybercrime.[25] There are several ways to classify cyber-crimes.[26] One way to classify cyber-crimes is to inquire whether computers make the fruit or instrumentalities of crime. In other words, the issue is whether the computer is a target of or a tool to commit the crime at issue.[27] Viruses, worms, Trojan horses, denial of service attacks are tools to maliciously destruct computer hardware and software and, therefore, are the cyber crimes of the first type. Such crimes did not exist before the creation of cyberspace. Online frauds and online child pornography are cyber crimes of the second type.[28] This type of cybercrime includes traditional criminal activities that have migrated to the Internet.[29]

The ability to conceal one's identity in cyberspace, or anonymity, makes it difficult to track a cyber criminal and thus provides an attractive medium to commit a cybercrime. There are no checkpoints or physical evidence.[30] A variety of legal and procedural issues arise when an investigation of a cybercrime requires gathering evidence across national

21. Albert I. Aldesco, *The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime*, 23 Loy. L.A. Ent. L. Rev. 81, § Introduction, ¶ 1 (2002).

22. O'Connor, *supra* n. 10, § The Varieties and Types of Cybercrime.

23. *Id.* at ¶ 4.

24. Krasavin, *supra* n. 2, at 2.

25. O'Connor, *supra* n. 10, § The Varieties and Types of Cybercrime.

26. *Id. See* Natalee Drummond and Damon J. McClendon, *Cybercrime – Alternative Models for Dealing with Unauthorized Use and Abuse of Computer Networks*, Law and the Internet ¶ 1 (2001).

27. O'Connor, *supra* n. 10, § The Varieties and Types of Cybercrime.

28. *Id.*

29. Testimony of James E. Farnan, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, on The FBI's Cyber Division, before the House Committee on Government Reform, Washington, D.C. <http://www.fbi.gov/congress/congress03/faran/051503.htm> (May 15, 2003).

30. Mark Grossman, *Cyberterrorism* <http://www.mgrossmanlaw.com/articles/1999/cyberterrorism.htm> (Feb. 15, 1999).

borders.[31]

C. CYBERATTACKS

Although humans have created cyberspace, the only residents in cyberspace are digital data – the ones and zeros and the inter-connected computers that store and transmit the data. Cyberspace is constantly under assault.[32] Cyber spies, thieves, saboteurs, and thrill seekers break into computer systems and networks, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, cyber-stalk, and harass individuals and companies.[33]

Many of the attacks are serious and costly,[34] but not violent. The ILOVEYOU virus and variants, for example, was estimated to have hit millions of users and cost billions of dollars in damage. The denial-of-service DOS attacks against Yahoo, CNN, eBay, and other e-commerce Web sites caused over a billion dollars in losses, and shook the confidence of business and individuals in e-commerce.[35]

The most recent and longest cyber attack was launched against Al-jazeera.net, the Arabic satellite news channel's Web site. The cyberattack lasted almost a week.[36] No one has ever sustained a crippling attack against a big Web site for so long.[37] The Federal Bureau of Inves-

---

31. Susan W. Brenner and Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. Marshall J. Computer & Info. L. 347 (2002). This article quoted Council of Europe, Convention on Cybercrime:

> One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is subject of a criminal investigation, thereby destroying the evidence.

Id. See International Guide to Combating Cybercrime, American Bar Association (2003).

32. *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*, 105 Cong. (May 23, 2000) (testimony of Dorothy E. Denning, Professor, Georgetown University) (available at <http://www.cs.georgetown.edu>). These attacks are facilitated with increasing powerful and easy-to-use software tools, which are readily available free from thousands of Web sites on the Internet. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. Hack attack on Al-Jazeera raises questions, <http://www.usatoday.com/tech/worls/iraq/2003-03—30-iraq-web_x.htm> (accessed May 19, 2003). Al-Jazeera countered by increasing its bandwidth to more than 100 time what an average corporation uses, but the attackers soon inundated the extra bandwidth. Al-Jazeera's technology manager stated: "No normal hacker can do that. We can't prove it, but we think for sure it's a big organization." *Id.*

37. *Id.*

tigation FBI monitored the hack but could do little to trace or stop it.[38]

D. THREAT OF CYBERTERRORISM

Cyberterrorism is the convergence of terrorism and cyberspace.[39] While "cyber", as explained in the foregoing text, is non-controversial, "terrorism" by nature is difficult to define.[40] As the old maxim goes: one man's terrorist is another man's freedom fighter.[41] Terrorism commonly involves violence between different moral cultures.[42] Everyone uses the word 'terrorism' to mean a kind of violence, of which he or she does not approve, and about which he or she wants something done.[43] In political rhetoric, terrorism involves killing, disruption, or destruction of something of value for political purposes by some one other than a government or its agents acting overtly. It is implied that the terrorist individual or group does not have conventional military or legal power to achieve its end.[44]

The U.S. Code defines "terrorism" as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[45] The Code specifies act, motive, actor and victim, but does not address the legality of the violence.[46]

The term cyberterrorism – comprising of "cyber" and "terrorism" was first coined in 1980s by Barry C. Collin, a senior research fellow at the Institute for Security and Intelligence in California.[47] Since then, term

---

38. *Id.*

39. Brenner, *supra* n. 31, at 1.

40. Krasavin, *supra* n. 2, at 1.

41. *Id.*

42. Theodore P. Seto, Article, *The Morality of Terrorism*, Symposium on Terrorism and Law, 35 Loy. L.A. L. Rev. 1227 (June 2002). Terrorists typically believe that they are engaged in a righteous cause; they believe that their acts are moral and justified. *Id.* at 1244.

43. *Id.* at n.13 (quoting Ileana M. Porras, *On Terrorism: Reflections on Violence and the Outlaw*, 1994 Utah L. Rev. 119, 124).

44. *Id.* at 1234 (e.g., Al Qaida, Hamas, or Chechnyan Liberation Front).

45. 22 U.S.C. § 2656f (2000). *See also* 22 U.S.C. § 2656f(d)(1) ("'international terrorism' means terrorism involving citizens or the territory of more than 1 country"); 22 U.S.C. § 2656f(d)(3) (" 'terrorist group' means any group practicing, or which has significant subgroups which practice, international terrorism"). For a more expansive definition, see *Threat of Terrorism in the United States*, Statement before the Senate Committee on Appropriations, Armed Services and Select Committee on Intelligence, 107th Cong. (May 10, 2001) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (available at <http://www.fbi.gov/congress/congress01/freeh051001.htm>).

46. *Id.* at 1233. Professor Seto points out that the U.S. Special Forces trained to operate clandestinely against economic targets would apparently constitute "terrorists" under this definition. *Id.*

47. Barry C. Collin, *The Future of CyberTerrorism: Where the Physical and virtual Worlds Converge*, 11th Annual International Symposium on Criminal Justice Issues, 15-18 (March 1997) (as quoted by Dorothy E. Denning, *Activism, Hacktivism and Cyberterrorism*:

"cyberterrorism" has been extensively used, if not overused. The term combines two greatest fears of this century: cyberspace and terrorism.[48]

Terrorism is, in fact, designed to be feared. That is its real power.[49] The technology is also feared not only because it is arcane and complex, but also because people believe that the computer technology has the ability to become the master, and humanity the servant.[50] The press has further fueled the fires by exaggerating the convergence – that one could destruct the physical world using a computer in his living room or cave.[51] According to Barry Collin, who created the term "cyberterrorism," there is a difference between mischievous hackers – the kind of people who break into government Web site to paint mustaches on official portraits – and CyberTerrorists:

> Like conventional terrorists, CyberTerrorists are out for blood. They try to do things like break into subway computer systems to cause a collision or use computers to tamper with power grids or food processing. However, unlike suicide bombers and roof-top snipers, CyberTerrorists attack from the comfort of home and can be in more than one place at a time through cyberspace. . . . CyberTerrorism can be far more damaging, and far more violent, than a 55-gallon drum of fuel and fertilizer. . . . CyberTerrorists' isolation from the results of their actions and the consequent lack of personal risk, make them particularly dangerous. . . . [T]he ease and low cost of CyberTerrorism combine to offer an attractive tool for once-conventional sociopaths.[52]

FBI's Mark Politt rebutted the foregoing by stating that computers are products of human being and offer immense benefits.[53] There are risks, but most risks are manageable. It is the "unmanageable" risks that we fear.[54]

The public was alerted to the "rise of cyberterrorism" even before September 11,[55] and the terrorist attacks of September 11 heightened the public fear of cyberterrorism.[56] The U.S. government has cited the Sri Lankan freedom fighters liberation group as the first group using

---

The Internet as a Tool for Influencing Foreign Policy <http://www.nautilus.org/info-policy/workshop/papers/denning.html> (accessed May 13, 2003)).

48. Mark M. Pollitt, *Cyberterrorism—Fact or Fancy?*, Proceedings of the 20th National Information Systems Security Conference, 285 (Oct. 1997).

49. *Id.* at 2.

50. *Id.* at 2.

51. *Id.* at 2.

52. Ames, *supra* n. 1.

53. Pollitt, *supra* n. 48, at 2.

54. *Id.*

55. Green, *supra* n. 4 (quoting Mr. George W. Bush during his presidential campaign that the "American forces are overused and underfunded precisely when they are confronted with a host of new threats and challenges – the spread of weapon of mass destruction, the rise of cyberterrorism . . .").

56. *Id.*

cyberterrorism, and, therefore, some claim that the U.S. government is prone to cyberterrorist attacks. However, experts argue that the Sri Lankan group's cyberattack in which the Sri Lankan embassy Web sites were put out of operation was not cyberterrorism, but rather a denial of service attack.[57] Experts deny that "we have seen cyberterrorism" and do not think that "we are going to see it for a couple of decades."[58] It is further claimed that

> [t]he closest thing that we have had is in Australia where someone hacked into a system and dumped sewage out into a bay. . . . It took him dozens of attempts and did not do that much damage. That is not terrorism. . . A network going down is not terrorism. Everyone who watched on September 11 knows what terrorism looks like. . . Your phone not working is not terrorism, that is annoyance. I would define cyberterrorism as using a computer to make planes fall out of the sky or building collapse. . . Shutting down of Wall Street happens every weekend. . . . I do not think that there is a way to completely shut down Wall Street. I won't argue that terrorists won't [wreak havoc]. I argue that whatever they may do does not involve computer networks, it will involve trucks and bombs, and airplanes. . . We can invent scenarios but they are not realistic. . . I don't see terrorism on computers. I just don't . . .[59]

Despite the lack of evidence, cyberterrorism is now considered a viable option for any individual or group.[60] The experts who anticipate a cyberterrorism attack on the United States are puzzled as to why cyberterrorism has not manifested itself yet.[61] Some possible reasons given are:

- Terrorists lack the computer expertise and have not recruited hackers.
- Leaders of the group may still be the product of a different, older worldview – one in which delivery method does not involve bits and bytes.
- Domestic extremists, and not the transnational groups, seem a likely source of cyberterrorism.
- It is some kid, or some disaffected adult, some technological Unabomber, that will strike and that will cause more damage

57. John Borland, *Analyzing the Threat of Cyberterrorism*, <http://www.techweb.com/wire/story/TWB19980923S0016> (Sept. 25, 1998) (quoting William Church).

58. Chris Conrath, It World Canada.com, *Secure Software? Don't hold your breath*, <http://www.itworldcanada.com/index.cfm/ci_id/33814.htm> (Oct. 4, 2002) (quoting Bruce Schneier, designer of the popular Blowfish encryption algorithm, CTO of counterpane Internet Security Inc.).

59. *Id. See* Green, *supra* n. 4, at ¶ 18.

60. Tara Mythri Raghavan, *In Fear of cyberterrorism: An analysis of the Congressional Response* ¶ 2, <http://www.jltp.uiuc.edu/recdev/articles/Raghavan/Raghavan.htm> (accessed May 23, 2003).

61. Brenner, *supra* n. 7.

than we ever thought possible.[62]

— Much of the nation's critical infrastructure operates on private networks that are not directly connected to the Internet—a fact which in and of itself—provides some level of protection.[63] Some financial institutions that allow online banking, are connected to the Internet and they are at risk.[64]

Because the computers are at the heart of American infrastructure —from storing information to adding in communications delivery—the government has stepped up to promote cyber security in order to prevent cyberterrorist attacks. In this regard, Congress passed the legislation, after the September 11 attacks, to protect the nation's information infrastructure from terrorism.[65] The Federal Acts and certain state laws cover cyber crimes, but do not define cyberterrorism.[66]

In addition to the Federal laws in effect, several states are considering passing legislation against cyber crimes and cyber attacks. As of December 2002, at least fourteen states have pending legislations that address cyberterrorism.[67] As it stands, the crime of cyberterrorism has been mentioned in certain statutes, but no governmental definition of cyberterrorism exists.[68] The State of New York has a pending legislation that defines cyberterrorism and makes cyberterrorism a crime.[69]

In spite of the fact that neither the Federal law nor any individual state law defines cyberterrorism, the term has been used in the literature in different ways. There is no consensus on the definition of, or on elements comprising, cyberterrorism. Some of the definitions are:

---

62. Brenner, *supra* n. 7 (quoting Bill Campbell, Mayor of Atlanta, Ga.).

63. Brenner, *supra* n. 7 (quoting Mr. Clark).

64. *Id.*

65. *Id.* The three pertinent Acts are:

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

The Cyber Security Act, which was signed into law on 11/25/02. This Act improves upon the Computer fraud and Abuse Act of 1986, and a part of Home Security package.

The Cyber Security Research and Development Act, a law promotes information technology research to address cyber security needs. *Id.*

66. 10 U.S.C.A § 2541 uses the phrase "prevention of cyberterrorism," and 10 U.S.C.A. § 509 uses the terms "crime activity (including cyberterrorism)" and "computer-related crime (including cyberterrorism)" without defining cyberterrorism. Similarly, a Kentucky statute uses the term "cyber terrorism." KRS § 39A 050.

67. National Conference of State Legislatures, *Cyberterrorism*, <http://www.ncslorg/lis/CIP/cyberterrorism.htm> (accessed May 22, 2003).

68. *See supra* n. 66.

69. Letter from Center for Democracy and Technology and Electronic Fronteir Foundation, to Governor George E. Pataki, <http://www.eff.org/privacy/TIA/20030314_letter_to_pataki.pdf> (accessed May 23, 2003) [hereinafter "letter"].

1) Cyberterrorism is hacking with body count[70]
2) Cyberterrorism is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives[71]
3) Cyberterrorism is any attack against an information function, regardless of the means[72]
4) Cyber-terrorism is defined as attacking sabotage-prone targets by computer that poses potentially disastrous consequences for our incredibly computer-dependent society[73]
5) Use of information technology as means by terrorist groups and agents is cyberterrorism[74]
6) Cyberterrorism can be defined as the use of information technology by terrorist groups and individual to further their agenda[75]
7) Cyberterrorism is premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents[76]
8) A bill passed by the New York Senate defines the crime of cyberterrorism as any computer crime or denial of service attack with an intent to . . . influence the policy of a unit of government by intimidation or coercion, or affect the conduct of a unit of government[77]

The first six definitions noted above are for general interest only as they are commentators' opinions. The seventh definition is a variation of the U.S. Department of State definition of terrorism.[78]

The last definition which is a part of the S. 1627, a bill passed by the New York Senate, will become the law in the state of New York upon signing by Governor George E. Pataki. Two groups that seek to promote civil liberties have opposed the proposed definition of cyberterrorism in the bill. The groups are: Center for Democracy and Technology,[79] and Electronic Frontier Foundation.[80] The groups are gravely concerned because S. 1627 defines the crime of cyberterrorism so broadly that even a

70. Krasavin, *supra* n. 2.
71. Denning, *supra* n. 32.
72. Goodman, *supra* n. 3 (quoting Rod Stark n. 77).
73. Krasavin, *supra* n. 2, at 1 (quoting an expert).
74. Krasavin, *supra* n. 2, at 2.
75. National Conference, *supra* n. 67.
76. Pollitt, *supra* n. 48.
77. Letter, *supra* n. 69.
78. Pollitt, *supra* n. 48 (quoting U.S. Department of State).
79. *See generally* <http://www.cdt.org>.
80. *See generally* <http://www.eff.org>.

very low-level, non-violent, minor, politically motivated computer crime would become a serious felony, if the bill were enacted into law.[81] The groups argue that the political protesters should not be treated as terrorists. The groups use "defacement" and "denial of service" attacks as two examples to illustrate how minor illegal acts in cyberspace will be treated as acts of terrorism under the proposed legislation.

Web defacement, where a Web site is entered without authorization and content is altered or replaced (but no permanent damage is done to the site), while illegal, is a non-violent disobedience tactic that is often intended precisely to affect the conduct of the government.[82] The groups contend that under the proposed legislation, the crime of Web defacement, now a class A misdemeanor, will be elevated to a terrorist felony. It raises a constitutional concern that S. 1627, if enacted, would more severely punish politically motivated web defacement than the same act for thrills or other non-political reasons.[83]

A denial of service [DoS] attack occurs when a network server is inundated with too many requests for information for it to handle so that legitimate users cannot access the server.[84] At present, a DoS attack is not considered a crime in New York. The bill S. 1627 makes any computer crime or "denial of service attack" a Cybercrime (and therefore a serious felony) if committed with the intent to . . . influence the policy of a unit of government by intimidation or coercion, or to affect the conduct of a unit of government. A DoS attack can be analogized to a "cyber sit-in" or a "cyber-blockade" a form of civil disobedience.[85] Another scenario is that a campaign that encourages citizens to send e-mail to their elected officials could be characterized as a DoS attack if the campaign results in a large volume of e-mail. The issue has been raised that the law that punishes the DoS attacks, when made to "affect the conduct of a unit of government" and does not punish them at all when done for non-political reason is likely to be found unconstitutional.[86]

II. CONCLUSION

The key element that differentiates cyberterrorism from terrorism is the use of cyberspace in carrying out a terror attack. The difference between cyberterrorism and other cyber attacks, such as hacking and cracking, is that the cyberterrorists are politically motivated, while other

81. Letter, *supra* n. 69.

82. *Id.*

83. *Id.*

84. Mark G. Milone, *Hacktivism: Securing the National Infrastructure*, 58 Bus. Law 383 (Nov. 2002).

85. Letter, *supra* n. 69.

86. *Id.*

cyber attackers have non-political motives. Cyberterrorism has not manifested itself primarily because of the lack of convergence that exists between the real and virtual worlds. Based on the current state of technology involving human intervention, there is little chance that it would manifest in the near future, if at all.

The federal and state laws at present do not define "cyberterrorism." Several states are considering making cyberterrorism a felony crime. Our society that prides itself on impartiality of law and justice faces a challenge to provide a clear and fair legislative guideline for dealing with cyberterrorism – a phenomenon that has not manifested itself until now and may never do so. In model cyberterrorism legislation, for a cyber crime to be elevated to cyberterrorism, the crime should, in addition to being politically motivated, result in violence against persons or property, or at least cause enough harm to generate fear in the population. Cyber attacks, perpetrated with political motivation, that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss, are the examples. Serious cyber attacks against critical infrastructures may be acts of cyberterrorism, depending on their impact. A cyber attack that disrupts the nonessential services or is mainly a costly nuisance should not be considered cyberterrorism.