

# **The Cyber-Intifada: Activism, Hactivism, and Cyber-Terrorism in the Context of the “New Terrorism”<sup>1</sup>**

**By Sean Lawson**

**[Prepared as a seminar paper for the course, Information Warfare and Security, taught by Dorothy Denning, Georgetown University, Fall 2001]**

## **Introduction**

With the fall of the Berlin Wall in 1989 and the collapse of the Soviet Union in 1991, the world passed from the relative simplicity of a bipolar world, in which nuclear annihilation was the ultimate threat to human security, into a seemingly new, more complex international system that lacked the same level of definition and predictability. The end of the Cold War unveiled a complex array of social, economic, and environmental issues that represent possible threats to international security but that had been masked by the dominance of the politico-military aspects of security during that period.<sup>2</sup>

Therefore, some analysts have begun to turn their attention toward what terrorism expert Bruce Hoffman calls more “exotic threats” such as bio-terrorism, agro-terrorism, and cyber-terrorism.<sup>3</sup> Lately, they are pointing to a new kind of threat to international security: the intentional use of computers, Internet, or other information technologies for

---

<sup>1</sup> The term “new terrorism” comes from Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (New York: Oxford University Press, 1999).

<sup>2</sup> See Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis*, (Boulder: Lynne Rienner, 1998) for a detailed analysis of the changes taking place in the field of security studies after the Cold War.

<sup>3</sup> Bruce Hoffman, “21<sup>st</sup> Century Terrorism has an all-too-Familiar Face,” *The Houston Chronicle*, (6 October 1999), A27; see also Bruce Hoffman, “Russian: Conventional Terrorism Still Works,” *The Los Angeles Times*, (26 September 1999), M2.

purposes of warfare or terrorism by other states or sub-state actors. Some refer to this new threat as “cyber-terrorism.”<sup>4</sup>

Recently, the discussion of cyber-terrorism has focussed in on events in the Middle East, where the Oslo Peace Process has broken down and violence has resumed between Palestinians and Israelis. A new dimension to this recent Intifada has been the use of Internet by both sides in the furtherance of their goals. Some have called this the “first full-scale war in cyberspace,”<sup>5</sup> and “the first example of a cyber-war between people fighting on the ground.”<sup>6</sup> One commentator speculates about the future impact of these recent events writing, “In the broader scheme of things, the Arab-Israeli cyber war offers a window into the kind of threats that leading economic powers will face in the twenty-first century. IT experts at the Pentagon have reportedly been preparing for precisely these kinds of attacks for years and are watching the situation closely.”<sup>7</sup>

Such proclamations indicate that recent events in the Middle East have further fueled pre-existing concerns by large and small countries alike that new information technology (IT), especially Internet, poses a dangerous new security threat. Therefore, one should do several things to accurately evaluate such claims by: 1) examining how in fact Internet has been used in the recent Intifada; 2) understanding the different types of

---

<sup>4</sup> There are actually many terms that address various different aspects of this threat. Others include: “cyber-war,” “info-war,” “net-war,” “info-terrorism,” or “cyber-crime.” They will be discussed in greater detail later in this paper.

<sup>5</sup> Bibi van der Zee, “The Editor: Weblife: The Week on the Net,” *The Guardian* (3 November 2000): 20.

<sup>6</sup> Kim Ghattas, “Net Casualties Mount in the First Web War,” *The Scotsman* (3 November 2000): 15.

<sup>7</sup> Gary C. Gambill, “Who’s Winning the Arab-Israeli Cyber War?” *Middle East Intelligence Bulletin* (November 2000); available at <http://www.meib.org>.

threats that may emerge from cyberspace; 3) comparing the Cyber-Intifada to these different threats; and 4) placing the Cyber-Intifada within the broader context of the “new terrorism.” A surprising picture will emerge, one in which the Cyber-Intifada fails to live up to its description as “the first war in cyberspace,” and may not even fit within the context of the “new terrorism,” which may in fact not be that new after all.

### **Cyber-Intifada<sup>8</sup>**

If it is true that recent events in the Middle East constitute the first, best example of cyber-war that one can point to, then it makes sense to first describe in detail what has been entailed in this cyber-war before moving to a more general discussion of definitional and theoretical issues related to cyber-terrorism, and before attempting to place cyber-terrorism within the context of the “new terrorism.”

This discussion will be broken up into several categories. First, the different types of attacks that have been used will be outlined. In order of least damaging to most damaging, they include: defacing attacks, directed denial of service attacks, viruses, and cyber-terrorism. Next, the reaction from policymakers to these recent attacks will be discussed, followed by general conclusions about the nature and effectiveness of the Cyber-Intifada.

#### *Defacing Attacks*

Defacing attacks occur when hackers break into a Web-site’s files and alter them by posting obscenities or generally changing the content of the site that is viewed on the World Wide Web. Most of the attacks involved in the Cyber-Intifada, whether

---

<sup>8</sup> I will use the term “Cyber-Intifada” as it fits more closely with the terminology being used to describe the physical conflict between Palestinians and Israelis of which this cyber-conflict is a direct outgrowth.

perpetrated by pro-Palestinian or pro-Israeli hackers, have involved some form of defacement. Some of the most notable include the defacement of the Hizbollah Web-site by Israelis at the beginning of the conflict.<sup>9</sup> Since that time many others have experienced such attacks, including the Iranian Ministry of Agriculture site,<sup>10</sup> the Web-site of Iranian President Mohammed Khatami,<sup>11</sup> the Anti-Defamation League site,<sup>12</sup> and the site of the U.S. high-tech firm Lucent Technologies because of their heavy business dealings in Israel.<sup>13</sup> Most notably, a hacker calling himself “Dr. Nuker,” a member of a group called the Pakistan Hackerz Club, perpetrated a more comprehensive and well publicized attack on the site of the American Israel Public Affairs Committee (AIPAC).<sup>14</sup>

#### *Distributed Denial of Service Attacks*

Defacing attacks are not that sophisticated and can usually be corrected quickly once the webmaster of the defaced site is informed of the problem. Distributed denial of service (DDoS) attacks entail flooding a site with e-mail or overwhelming it with requests for information which block others’ access to the site and/or cause the site to crash. These types of attacks have also been very popular recently. In addition to defacement, the sites of Hizbollah, Hamas, and the Palestinian Information Center have

---

<sup>9</sup> Noah Adams and Linda Gradstein, “Cyberattacks on Key Israeli Web-Sites,” *All Things Considered* (26 October 2000).

<sup>10</sup> Gwen Ackerman, “E-Jihad Continues, Israelis Hit Iranian Ministry,” *The Jerusalem Post* (6 November 2000).

<sup>11</sup> “Cyber Terrorism: Cyber Wars: The Palestinians Strike Back,” *National Journal’s Technology Daily* (26 October 2000).

<sup>12</sup> “ADL Reacts to Attack on its Web Site,” *U.S. Newswire* (27 December 2000).

<sup>13</sup> Charles Molineaux and Dan Verton, “Cyber Terrorism Threat in Middle East, CNNfn,” *The N.E.W. Show* transcript # 00111703FN-107 (17 November 2000) and Bill Maxwell, “Middle East War Rages on the Internet,” *St. Petersburg Times* (29 November 2000).

fallen prey to DDoS attacks.<sup>15</sup> Several Israeli government sites have been shut down through DDoS attacks including sites for the Israeli Knesset, the Foreign Ministry, the Israeli Defense Force, and the main government site. Israelis have said that these attacks have caused no serious damage beyond being an annoyance. No sensitive information or infrastructure systems are connected to the publicly accessible Internet, they say.<sup>16</sup>

### *Viruses*

As Israeli officials have said, both of these types of attacks may constitute annoyance more than anything. The next level of attack that may be more serious would be the use of computer viruses. Though there have been reports of the use of a Trojan Horse virus and other, more sophisticated attacks, no direct evidence exists to indicate that this is the case.<sup>17</sup> Of course, there are several caveats to keep in mind here. First, the greater level of knowledge needed to carry out such attacks may have made them less attractive. Second, the inability to control the impacts of such an attack once it is released (i.e. the virus may come back to affect the perpetrator) may be a deterrent factor. But, third, even if an effective, targeted attack with a virus was carried out, governments may not be willing to admit that they had been the victim of a successful attack so as not to allow the perpetrator knowledge of his or her success, thereby increasing the risk of future attacks. So, there may be powerful deterrent factors for one who would perpetrate

---

<sup>14</sup> John Schwartz, "Hacker Defaces Pro-Israel Web Site," *The New York Times* (3 November 2000).

<sup>15</sup> "Arab Hackers Retaliate Israeli Cyber Attacks," *Al-Bawaba* (26 October 2000); available from <http://www.albawaba.com>.

<sup>16</sup> *Ibid.*, Adams and Gradstein, and "Cyber-Attacks Against Israeli Sites Escalate," *Xinhua General News Service* (26 October 2000).

<sup>17</sup> "iDefense: Middle East Tensions Move Online; Pro-Israeli and Pro-Palestinian hackers Taking Down Web Sites, Threatening to Escalate Cyber War Tactics," *Business Wire* (31 October 2000).

such an attack. Finally, such an attack, even if it were successful, may never become known.

### *Cyber-terrorism*

Another category of attack that has been prevalent involves the stealing, corruption, or alteration of information contained on a particular site. These acts can have actual, damaging impacts on people or institutions in cyber-space and in the physical world. This may come closest to what will be defined later as “cyber-terrorism.” A mild example is the incident in which key files were erased from the Knesset’s Web-site because it involved the destruction of information contained there, although it did not cause very serious impacts.<sup>18</sup> Threats by pro-Palestinian hackers, if carried out, to attack major e-commerce sites in the U.S. in response to Israeli hacker attacks, may fit within this category.<sup>19</sup> The attack perpetrated against AIPAC by Dr. Nuker mentioned above comes even closer because, in addition to defacement, 3,500 email addresses were stolen, anti-Israeli messages were sent to these addresses, and 700 credit card numbers were stolen and subsequently posted on Dr. Nuker’s Web-site. The victims were forced to cancel their cards, although no physical or financial damage was reported.<sup>20</sup> In apparently the most organized attempt yet, a pro-Palestinian group with ties to Hizbollah calling itself Unity, devised a plan of attack comprised of four phases. Phase one involved crashing Israeli government sites. Phase two involved hitting the Bank of Israel and Tel Aviv stock market. Phase three involved targeting Israeli Internet service

---

<sup>18</sup> Joshua Brilliant, “Hackers Shut Israel Government Internet Sites,” *United Press International* (26 October 2000).

<sup>19</sup> Molineaux and Verton.

<sup>20</sup> John Schwartz, “Hacker Defaces Pro-Israel Web Site,” *The New York Times* (3 November 2000).

provider (ISP) infrastructure, including the Israeli Golden Lines company and U.S. based Lucent Technologies. Finally, phase four was to include destruction of Israeli e-commerce sites. It is important to note that, to a greater or lesser degree, all of these phases have been achieved except for phase four.

Finally, only two incidents may actually meet the full definition of cyber-terrorism. This will include purposeful targeting of information resources in the physical world or use of corruption or destruction of information resources to cause physical damage. The Israeli targeting of the Voice of Palestine radio and television is an example. One interesting example is the case in which a Palestinian woman used a chat-room to lure an Israeli teenage boy to a rendezvous point where he was kidnapped and murdered.<sup>21</sup> In this regard, info-terrorism constitutes a coming together of terrorist activities and tactics old and new.

#### *Policy Response*

There have been interesting policy responses in the U.S. and Israel as a result of these attacks. The U.S. National Infrastructure Protection Center, an F.B.I. program, has become involved by sending out warnings that U.S. sites could be hit.<sup>22</sup> For its part, the IDF was forced to open a new site on AT&T after its site administered by Israeli NetVision was shut down.<sup>23</sup> Seeing the potential for such attacks, experts from the U.S. and Israel met a year prior to the recent violence, in November 1999, and agreed to cooperate in countering cyber-terrorism and chemical and biological weapons (CBW)

---

<sup>21</sup> "Arab Woman Admits Luring Israeli in Internet Death," *Reuters* (26 February 2001); available from [http://www.infowar.com/class\\_3/01/class3\\_022601a\\_j.shtml](http://www.infowar.com/class_3/01/class3_022601a_j.shtml).

<sup>22</sup> "Cyberwar Heating up in Middle East: U.S.," *Agence France Presse* (27 October 2000).

<sup>23</sup> Adams and Gradstein.

terrorism by working to develop new technologies and by sharing intelligence.<sup>24</sup>

Additionally, the chairman of the Knesset Internet Committee, Michael Eitan, has called for an international treaty in which member countries would pass and enforce similar anti-hacking laws. As part of the treaty regime, he calls for the use of sanctions against countries that do not prosecute hackers. Finally, where Israel in particular is concerned, he calls for a national authority for computer defense.<sup>25</sup>

Of course, on the part of some international actors, a policy response could be of a more offensive nature. The German Federal Intelligence Service says that governments around the world are training hacker soldiers for the purposes of harassing opponents, espionage, and attacks on vital infrastructures.<sup>26</sup>

Arabs have begun to think about the possible, future policy implications of the Cyber-Intifada as well. Mizra Asrar Baig, a Middle East Internet security consultant, has expressed misgivings about Arabs' ability to secure themselves against potentially serious, coordinated, and damaging reprisals by Israelis in the future. He argues that, compared to the amount of expertise that Israelis have in computer technology and hacking, Arab hackers are amateurs. Their attacks, he argues, only leave a trail of activities that end up helping the Israeli hackers in the long run. Such attacks give Israel the incentive not only to improve its security but also reason to retaliate. Unfortunately for Arabs, the Israelis know where and how to target their attacks because many Middle

---

<sup>24</sup> Aluf Benn, "Israel, U.S. Join to Fight Cyber-Terror," *Ha'aretz* (12 October 1999).

<sup>25</sup> Gwen Ackerman, "MK Eitan Calls for International Pact to Stop Cyber Warfare," *The Jerusalem Post* (2 November 2000): 4.

<sup>26</sup> "Internet: a New Battlefield for the World's Wars," *Al-Bawaba* (6 November 2000); available from <http://www.albawaba.com>.

East networks rely on the firewall software called Checkpoint which is an Israeli produced product that Israelis not doubt know how to defeat. He says, for example, that this is the case in Saudi Arabia where recently it has been noticed that Saudi networks have been scanned by someone looking to gather information about the network's information infrastructure. This could be Israeli hackers gathering information for use in a future attack. As vulnerabilities become apparent, attacks can become potentially more devastating, he argues. This is especially the case in Saudi Arabia, where he claims that ninety-nine percent of organizations have no security in place to detect scanning.<sup>27</sup>

### *Observations and Conclusions*

Several general observations and conclusions can be made of the recent confrontation in cyber-space:

- The scope of the conflict in cyber-space has been more far-reaching than the physical conflict, including attacks to and from the U.S., Israel, Palestine, Egypt, Lebanon, Jordan, and Pakistan, and others, along with some neo-Nazis becoming involved against Israel. The base of participation has included not just hackers but average people, especially young people, participating from personal computers in the home or from Internet cafes.<sup>28</sup>
- The wide distribution of participation, with little hierarchical coordination of efforts, has favored the Palestinians by diminishing the risk of direct retaliation by the Israelis because the threat is essentially nebulous. This may make the fact that

---

<sup>27</sup> Molouk Y. Ba-Isa, "Cyber War Could be Costly for Arabs," *Middle East Newsfile* (26 December 2000).

<sup>28</sup> "Cyber Warfare Thrives in Israel-PA Conflict," *Middle East Newslines* (18 October 2000); Joshua Brilliant, "Hackers Shut Israel Government Internet Sites," *United Press International* (26 October 2000); and Lee Hockstader, "Pings and E-Arrows Fly in Mideast Cyber-War," *The Washington Post* (27 October 2000): A01.

Israel is the most computer literate, connected country in the Middle East more of a liability than an asset as it presents a greater target for a wide-spread, dynamic adversary.<sup>29</sup>

- It may be difficult to define actors clearly and accurately in cyberspace. An example unrelated to the Cyber-Intifada illustrates this most clearly. The U.S. believed that it was undergoing repeated cyber-attacks by the Falun Gong religious organization in New York. It was eventually discovered that the attacks emanated from the Chinese Ministry of Public Security as an attempt to discredit the opposition religious group.<sup>30</sup> The involvement of different groups from all over the world, and the possibility for the future involvement of hackers-for-hire<sup>31</sup> or hacker thrill-seekers suggests that defense as well as offense in cyberspace may prove difficult at best for institutions which are rigid and hierarchical.<sup>32</sup>
- There exists the potential for important system-effects<sup>33</sup> to develop which will be important to the shape and flow of cyber-conflicts. For example, publicity is important for attacks such as DDoS attacks to succeed because they require

---

<sup>29</sup> Joshua Brilliant, "Hackers Shut Israel Government Internet Sites," *United Press International* (26 October 2000) and Gary C. Gambill, "Who's Winning the Arab-Israeli Cyber War?" *Middle East Intelligence Bulletin* (November 2000); available at <http://www.meib.org>.

<sup>30</sup> "Internet: a New Battlefield for the World's Wars," *Al-Bawaba* (6 November 2000); available from <http://www.albawaba.com>.

<sup>31</sup> Bill Maxwell, "Middle East War Rages on the Internet," *St. Petersburg Times* (29 November 2000): 17A.

<sup>32</sup> "Internet: a New Battlefield for the World's Wars," *Al-Bawaba* (6 November 2000); available from <http://www.albawaba.com>; see also John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996).

<sup>33</sup> For more discussion of "systems-effects" and the nature of complexity see, Robert Jervis, *Systems-Effects: Complexity in Political and Social Life* (Princeton: Princeton University Press, 1997) and Robert Axelrod and Michael D. Cohen, *Harnessing Complexity: Organizational Implications of a Scientific Frontier* (New York: The Free Press, 1999).

participants to visit a particular Web-site and click on a command button that will initiate an attack. However, this necessary publicity causes ISPs to find the attack sites and remove them, essentially what could be considered a negative feedback loop. Evolutionary processes may be observed also. “Israeli Internet services may well be made more resilient as a result [of attacks], and the companies that advise on defensive systems will get richer.”<sup>34</sup> One can think of the way in which some bacteria have developed resistance to standard antibiotics as a similar process. Potential for positive feedback loops exists as well. “Sympathetic hackers and others around the world are likely to begin offering their services and jumping into the fray as the high-profile nature of the conflict continues to grow.”<sup>35</sup> With the interaction of both positive and negative feedback loops and evolutionary processes, one can begin to see the potential for unpredictable, dynamic outcomes.

- Finally, for all the hype and fear expressed over the recent “cyber-war,” not much has been accomplished except that some have gained a sense of participation and some may have been diverted from more violent activities. If a “victory” had to be assigned, it would go to the Palestinians with more offensive

---

<sup>34</sup> Brian Whitaker, “Online: War Games on the Net: But This Time it’s for Real,” *The Guardian* (30 November 2000): 6.

<sup>35</sup> “iDefense: Middle East Tensions Move Online; Pro-Israeli and Pro-Palestinian hackers Taking Down Web Sites, Threatening to Escalate Cyber War Tactics,” *Business Wire* (31 October 2000).

Web-site hacks than the Israelis thus far.<sup>36</sup> Yet, this seems a crude method for deciding victory in this case. The situation appears to be a stalemate if anything.

### **The Cyber-Intifada Redefined**

Placing the Cyber-Intifada into the larger discussion of cyber-terrorism shows that it is in fact not cyber-terrorism or cyber-war. Dorothy Denning identifies three types of activity in cyberspace: activism, hacktivism, and cyber-terrorism.

Activism in cyber-space is the “normal, non-disruptive use of the Internet in support of an agenda or cause.” Hacktivism is more serious and “refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a target’s Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are Web sit-ins and blockades.” Finally, she defines cyber-terrorism as “the convergence of cyberspace and terrorism. It covers politically motivated operations intended to cause grave harm such as loss of life or severe economic damage.”<sup>37</sup>

It appears that the Cyber-Intifada, with the few exceptions mentioned above, fits better in the category of hacktivism than it does within the category of cyber-terrorism. Additionally, if one wanted to think of cyber-war as existing at the state level only, then the Cyber-Intifada would certainly not fit that category either.

---

<sup>36</sup> Brian Whitaker, “Online: War Games on the Net: But This Time it’s for Real,” *The Guardian* (30 November 2000): 6; Richard Sale, “Mideast Conflict Roars into Cyberspace,” *United Press International* (7 December 2000).

<sup>37</sup> Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy,” (The Terrorism Research Center, 1999); available from <http://www.terrorism.com/documents/denning-infoterrorism.html>.

The four basic goals of hacktivism are to: 1) deny access to data, 2) disrupt or destroy data, 3) steal data, or 4) manipulate data.<sup>38</sup> The tools of hacktivism should sound familiar now that the details of the Cyber-Intifada have been examined. They include the use of virtual sit-ins and blockades. These can be achieved through the DDoS attacks discussed above. E-mail bombs are another method. This involves flooding a site with e-mail messages so that the system crashes. Additionally, hacktivists can use Web hacks and computer break-ins to steal and/or change information on a site. Finally, computer viruses or worms can be used, both pieces of code that can be used to damage computer networks.<sup>39</sup>

To properly understand the possible implications of cyber-terrorism it is necessary to not only look at vulnerabilities to such attacks, but also to the capabilities and motives of those who may perpetrate such an attack. Of vulnerabilities, Denning argues that most critical infrastructure has enough human involvement built in that the threat of a devastating cyber-terror attack is not as high as previously believed.<sup>40</sup> Yet, there are some advantages for the perpetrator of a cyber-terror attack. It can be perpetrated from a remote location; it is relatively cheap; it is not physically dangerous; and it can generate a great deal of media coverage.<sup>41</sup>

---

<sup>38</sup> W. Hutchinson, "Concepts in Information Warfare," *Journal of Information Warfare* [demo article]; available from <http://www.mindsystems.com.au>.

<sup>39</sup> Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism."

<sup>40</sup> This is ironic, of course, because the main reason for creating many of the automated, computerized systems that we now depend on was to decrease the risk of human error leading to devastating accidents. Now, we find that the presence of humans in these systems is essential for decreasing their vulnerability to cyber-terror attacks. This further strengthens the argument that the relationship between humans and technology is a complex, dynamic, and evolutionary system. For more on this idea see Edward Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences* (New York: Vintage Books, 1996).

<sup>41</sup> Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism."

Denning outlines three levels of capability for groups pursuing cyber-terror:

- **Simple-Unstructured:** The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.
- **Advanced-Structured:** The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.
- **Complex-Coordinated:** The capability for a coordinated attack causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability.<sup>42</sup>

The capabilities displayed during the Cyber-Intifada are clearly at the level of “Simple-Unstructured” attacks. The attacks have not risen to the level of cyber-terrorism for the most part, and certainly not cyber-war, nor have the attacks been that sophisticated either.

Who might perpetrate a sophisticated cyber-terror attack? Some believe that extremist religious groups who would be more likely to perpetrate WMD terrorism may also be the groups who would be most likely to have the motivation to perpetrate a sophisticated cyber-terror attack. However, there may be a break between motivation and skill level that would prevent such an attack. Denning writes, “While many hackers have the knowledge, skills, and tools to attack computer systems, they generally lack the motivation to cause violence or severe economic or social harm. Conversely, terrorists who are motivated to cause violence seem to lack the capability to cause that degree of damage in cyberspace.” She writes further of hackers, explaining that, “hacker groups

---

<sup>42</sup> Dorothy E. Denning, “Cyberterrorism,” Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives (23 May 2000); available from <http://www.terrorism.com/documents/denning-testimony.shtml>.

are psychologically and organizationally ill-suited to cyber-terrorism, and that it would be against their interests to cause mass disruption of the information infrastructure.”<sup>43</sup>

Walter Laqueur, in his discussion of “new terrorism,” speaks briefly of cyber-terrorism, expressing many of the same concerns that Denning has expressed. Yet, in the end, he identifies a different type of threat, one that may be more primitive, but ultimately more effective and more suited to the terrorist’s goals. He explains that,

In the future, terrorist action aimed at information technology will continue to be destructive, but on a primitive level. Society is becoming much more vulnerable, and the places of greatest vulnerability are well known. Guerrillas in deepest Mexico and Columbia have been destroying high-voltage transmission lines. Power stations in Bosnia and elsewhere have been frequent targets. The consequences are that society can be shut down for hours, sometimes days...However, such operations will not add to the popularity of a terrorist gang, nor will it translate into political power. But it may fit the program of the pan-destructionists.<sup>44</sup>

Indeed, Laqueur sees cyber-terrorism not as a threat by itself, but as having value only within the context of the “new terrorism.” He largely rejects the idea of a purely “cyber” form of cyber-terrorism, arguing here that the real threat will be the use of physical means of destruction against an information infrastructure by the same people who would perpetrate such acts as WMD terrorism. Therefore, it is to the “new terrorism” in general that we now turn, examining the Cyber-Intifada and cyber-terrorism’s proper place within this context.

### **Cyber-Intifada and the New Terrorism**

It is important to understand that fear over cyber-terrorism and cyber-warfare has arisen within the context of what is called the “new terrorism,” as mentioned previously.

---

<sup>43</sup> Ibid.

<sup>44</sup> Laqueur, 262-263.

Worry over a potentially dangerous intersection between new technologies and terrorism is a theme that runs through concern over potential WMD terrorism as well as cyber-terrorism. Robert Jay Lifton writes; “It is not true that there is nothing new under the sun. To be sure, the oldest human emotions continue to haunt us. But they do so in new settings with new technology, and that changes everything.”<sup>45</sup>

Concern over possible CBW terrorism reached governments and citizens around the world on the morning of 20 March 1995 when several members of the Japanese religious cult, Aum Shinrikyo, released sarin nerve agent on five different subway trains in Tokyo by puncturing plastic bags containing the agent. The action, believed to aid in the fulfillment of Aum’s prophecy of an Armageddon-type battle between the United States and Japan, resulted in twelve deaths and thousands of injuries.<sup>46</sup> Since that time, much attention has been focussed and much government money has been spent on assessing and combating the threat of WMD terrorism.<sup>47</sup> With the discovery of Iraq’s advanced chemical and biological warfare programs by U.N. weapons inspectors following the Gulf War and revelations by former deputy director of the Soviet biological weapons program, Ken Alibek—who defected in 1992—that the Soviets had established

---

<sup>45</sup> Robert Jay Lifton, *Destroying the World to Save it: Aum Shinrikyo, Apocalyptic Violence, and the New Global Terrorism*, (New York: Metropolitan Books, 1999), 3.

<sup>46</sup> Tim Ballard, Jason Pate, Gary Ackerman, Diana McCauley, and Sean Lawson, “Chronology of Aum Shinrikyo’s CBW Activities,” *Center for Nonproliferation Studies Reports* (Monterey: Monterey Institute of International Studies, 2001); available from [http://cns.miis.edu/pubs/reports/aum\\_chrn.htm](http://cns.miis.edu/pubs/reports/aum_chrn.htm).

<sup>47</sup> Shortly after the arrest of Shoko Asahara in May 1995, a hearing was conducted in October to look at the threat of WMD terrorism in light of Aum. Permanent Subcommittee on Investigations, Committee on Government Affairs, U.S. Senate hearing, staff statement, “Global Proliferation of Weapons of Mass Destruction: A Case Study on Aum Shinrikyo,” *Global Proliferation of Weapons of Mass Destruction, Part I*, 31 October 1995 (Washington D.C.: Government Printing Office, 1996). President Clinton’s FY2000 budget proposes \$10 billion dollars for counterterrorism, up from \$6.7 billion the previous year, largely due to the threat of WMD terrorism. Henry L. Hinton, Testimony Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on

the most advanced offensive biological weapons program in the world, despite Soviet ratification of the Biological and Toxin Weapons Convention of 1972, the world could no longer ignore the threat of CBW terrorism. The fact that Aum had developed a fairly sophisticated CBW capability and carried out an attack with absolutely no warning from the U.S. intelligence community worried U.S. lawmakers, especially considering that the U.S. was identified by Aum as one of its major enemies.<sup>48</sup> Recent events in the Middle East may lead to a similar effort in regard to cyber-terrorism.

History is replete with examples of states and sub-state groups using chemical and biological agents in warfare and/or terrorist actions.<sup>49</sup> Though Walter Laqueur is certainly correct when he observes that terrorism is inherently difficult to define or to make generalizations about, as many terrorist groups have existed in widely varying situations with different ideologies, leadership, and resources, there is the need to define and make generalizations nonetheless.<sup>50</sup> Indeed, a broad look at terrorism throughout history can

---

Government Reform, House of Representatives, *Combating Terrorism: Observations on the Threat of Chemical and Biological Terrorism*, (GAO: 20 October 1999), 2.

<sup>48</sup> Permanent Committee on Investigation, 5-7.

<sup>49</sup> See George W. Christopher, Theodore J. Cieslak, Julie A. Pavlin, and Edward M. Eitzen, Jr. "Biological Warfare: A Historical Perspective," *Biological Weapons: Limiting the Threat*, Ed. Joshua Lederberg (Cambridge: MIT Press, 1999); W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the Twentieth Century*, Working Paper (Washington, D.C.: Center for Counterproliferation Research, 1998; Ron Purver, *Chemical and Biological Terrorism: The Threat According to the Open Literature*, Canadian Security Intelligence Service, unclassified (June 1995); *The RAND-St. Andrews Terrorism Chronology: Chemical/Biological Incidents 1968-1995*, (St. Andrews College, Cambridge University); and *WMD Terrorism Database Project*, Center for Nonproliferation Studies, Monterey Institute of International Studies, <http://cns.miis.edu>.

<sup>50</sup> Laqueur, 46.

lead to helpful generalizations. Martha Crenshaw writes, “Yet terrorist activity considered in its entirety shows a fundamental unity of purpose and conception.”<sup>51</sup>

Use of CBW agents for terrorist purposes may not be as new as we think. Additionally, because traditional terrorist groups have shown interest in CBW, it is not accurate to say that new technologies necessarily lead to changes in terrorist tactics or motives. Yet, at the same time, some have correctly observed that a shift has occurred in terrorist tactics and motives over the past few years, whether those groups are relying on new weapons or information technologies or more traditional methods. If anything, new weapons and information technologies may allow terrorists more options and flexibility in pursuing their goals.

Bruce Hoffman makes three core distinctions between more “traditional” terrorist groups and newer religious terrorist groups such as Aum. In fact, Aum may provide the most extreme example seen so far. First, Hoffman argues that these new groups differ from the old in that violence becomes an end in and of itself, a sacred duty with theological significance.<sup>52</sup> Second, unlike traditional terrorist groups who are claiming to represent a particular constituency within society and attempting to attract new members for that constituency, many religious terrorist groups represent no one other than themselves.<sup>53</sup> Third, terrorist groups have traditionally used violence as a means to affect a change in the status quo or foment a popular movement to replace the status quo. Newer religious terrorists suffer from a sense of alienation; they are outsiders. This

---

<sup>51</sup> Martha Crenshaw, “The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice,” *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. Ed. Walter Reich, (Washington D.C.: Woodrow Wilson Center Press, 1990), 10.

<sup>52</sup> Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 94.

<sup>53</sup> *Ibid.*, 94-95.

leaves the available pool of targets and enemies wide open for the religious terrorist, leading to the possibility of much greater violence.<sup>54</sup>

Looking at each of these three characteristics leaves one unconvinced that cyber-terrorism fits within this framework. First, one notices that for all the focus on new technologies, when it comes to ultimately characterizing and defining the “new terrorists,” attention shifts to factors related specifically to the *people* involved. Indeed, terrorism of any kind is a human endeavor. One should question whether or not the people who could become involved in a cyber-terror attack fit the description of the “new terrorists,” their motives, and their tactics.

Second, if violence is an end in and of itself, then it seems that cyber-terrorism does not fit the requirement. Physical attacks against information infrastructure may come closer, but still lack the tendency toward mass, physical destruction of civilian populations. The use of indiscriminate, highly effective computer viruses, or the hacking of critical infrastructure systems to cause mass chaos or disruption of economies may come close as well. But, just like CBW attacks, these tactics have the potential to be uncontrollable and to come back to visit their impacts on the perpetrators as well.

Third, those becoming involved in cyber-terror activities may fit Hoffman’s description of people not representing a particular constituency within society or attempting to attract new members for that constituency. The observation that in the recent Cyber-Intifada hackers-for-hire, or bandwagon, thrill-seekers, may have become involved may be an example. Yet, the opposite may be true as well. Certainly, in this case, there is a core constituency that is being represented on both sides. Cyber-terrorist

---

<sup>54</sup> Ibid., 95.

tactics may not lend themselves to only one type of terrorist, as is the case with CBW as well.

Fourth, if Hoffman is correct that newer terrorist groups suffer from a sense of alienation that makes the world a larger, target-rich environment, leading to greater violence, then the potential for cyber-terrorism could be viewed in two different ways. One could argue that cyber-terrorism is a tactic for those who want to have an impact but who do not want to resort to violence. Therefore, these new, more potentially violent groups will have no use for a tactic that is relatively passive compared to mass, physical violence. Yet, one could take the opposite side by arguing that because the whole world is a target and nothing is exempt, such groups may be more willing to try new technologies and tactics, whatever they may be. There has just not been enough experience with these new groups or with cyber-terror, let alone a combination of the two, to be able to know what the case will be. There should be no doubt that there will likely be no one standard case, as the peculiarities of particular individuals and groups will combine with new capabilities to produce unexpected outcomes.

## **Conclusion**

By examining the details of the Cyber-Intifada, one comes to the conclusion that this has not been a full-scale war in cyberspace. With the exception of a few cases that may legitimately be called cyber-terrorism, most of what has occurred may be more accurately described as hacktivism. Viewed in terms of the theoretical, speculative literature on the subject, the Cyber-Intifada indicates that the world has yet to experience the worst of what scholars believe may be possible in the future. Viewed in the context of the “new terrorism” and terrorists, the Cyber-Intifada fails on several counts. The

attacks have been in support of a particular conflict, in support of and perpetrated by particular constituencies, and specifically targeted at assets and resources viewed as directly connected to one or the other side. The central theme that connects the “new terrorism” with cyber-terrorism is the use of new technologies. Yet, this by itself is not enough to link the two in one category for analysis. Indeed, use of CBW by terrorist groups may not be as new as we are told. Those who would use one type of technology or tactic may not be the same in all cases. Terrorist tactics and motives may not be so much driven by technology as the development and incorporation of new technologies is driven by other factors within these groups.

This study should not undermine a sense of healthy anxiety about the potential for cyber-terrorism to have serious effects in the future. However, a more realistic and critical view of the Cyber-Intifada is healthy as well. We should be clear with our definitions of key terms, especially those related to identifying the levels of threat and forms that cyber-attacks may take. Finally, fascination with new technology, a sense of technological determinism, or technological optimism should not unduly influence research into these issues. We should not be caught with our heads in the sand; nor should we be caught with our heads in the clouds, being swept along by a current of emotionalism and fear.