A View of Cyberterrorism Five Years Later

Dorothy E. Denning
Center on Terrorism and Irregular Warfare
Naval Postgraduate School

[Chapter 7 in *Internet Security: Hacking, Counterhacking, and Society* (K. Himma ed.), Jones and Bartlett Publishers, 2007.]

A few weeks after the September 11 terrorist attacks, the Pakistani Muslim hacking group GForce Pakistan announced the formation of the "Al-Qaeda Alliance Online" on a U.S. government website it had just defaced. Declaring that "Osama bin Laden is a holy fighter, and whatever he says makes sense," the group posted a list of demands and warned that it planned to hit major U.S. military and British websites.[1] Another GForce defacement contained similar messages along with heart-wrenching images of badly mutilated children said to have been killed by Israeli soldiers. A subsequent message from the group announced that two other Pakistani hacking groups had joined the alliance: the Pakistan Hackerz Club and Anti India Crew. Collectively, the groups had defaced hundreds of websites, often with political messages.

Was this a sign that al-Qa'ida had acquired a hacking unit bent on causing cyberterror – or just another group of hackers expressing themselves on public websites while trying to impress their peers? In this case, it looked more like the latter. On October 27, GForce wrote on a defaced U.S. military website that it was "not a group of cyber terrorists." Condemning the attacks of September 11 and calling themselves "cyber crusaders," they wrote, "ALL we ask for is PEACE for everyone." This was among their last recorded defacements. GForce Pakistan and all mention of the Al-Qaeda Alliance Online disappeared.

The possibility of cyberterrorism, however, remains a concern, as Al-Qa'ida and other terrorist groups have become increasingly aware of the value of cyberspace to their objectives. They have become adept at using the Internet to distribute propaganda and other information, collect data about potential targets and weapons, communicate with cohorts and supporters, recruit, raise money, and generally facilitate their operations. They have advocated conducting cyber attacks and engaged in some hacking. New hacking groups have emerged with apparent ties to terrorists. Even if the Al-Qaeda Alliance Online does not pose a threat of cyberterror, others might.

The purpose of this article is to assess the cyberterror threat, particularly from al-Qa'ida and the global jihadists who are part of the broader social movement associated with al-Qa'ida. As such, the view offered here supercedes that which I presented about five years ago, first to the Special Oversight Panel on Terrorism of the Committee on Armed Services in the U.S. House of Representatives in May 2000[2] and then in an article written shortly after the September 11 attacks in 2001.[3] This assessment was based primary on speculation of what terrorists would likely be interested and capable of achieving. My

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A View of Cyberterrorism Five Years later	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Center of Terrorism and Irregular Warfare,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
pre-publication version Readings in Internet Security: Hacking, Counterhacking, and Society (K. Himma ed.), Jones and Bartlett Publishers, Boston, 2006

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**18**	

overall conclusion was that at least for the time being, bombs posed a much greater threat than bytes, but we should not shrug off the threat.

The assessment offered in this paper is based less on speculation and more on indicators of cyberterror. These are pieces of evidence that demonstrate a capability or intent to conduct cyberterror. The ones I have found so far range from the actual conduct of cyber attacks to other types of activities that show at least some capability or intent. The indicators are grouped into five categories, and each category examined in terms of the evidence found so far.

While this paper evaluates the threat of cyberterror, it does not attempt to evaluate its risk. To assess the cyberterror risk, one must consider not only the capabilities and motives of terrorists (the threat), but also the vulnerability of critical information systems to attack. Without such vulnerabilities, there is no risk. This paper does not address the vulnerability side of risk, and hence does not evaluate the likelihood of cyberterror operations succeeding. Hence, it only addresses half of the risk equation.

Before offering my current assessment, I will discuss what cyberterror is and is not. I will also review two studies of cyberterror conducted by the Center on Terrorism and Irregular Warfare at the Naval Postgraduate School in 1999 and 2000, before my arrival in late 2002. Although the studies are now over five years old and summarized in my earlier writings, my goal for the current paper is to provide a fairly complete assessment of the threat side of cyberterror.

What is Cyberterrorism?

Cyberterrorism is generally understood to refer to highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction and disruption against digital property.

Cyberterrorism is distinguished from cyberwar in that the former comprises acts performed by non-state actors, whereas the latter consists of government activity. With cyberwar, a state's military engages in cyber attacks against an adversary within the context of a declared war.

Although cyberspace is constantly under assault by non-state actors, the attacks so far are generally not considered to be acts of cyberterrorism. They fall short for two reasons. First, the attacks that are the most destructive and generate the most fear are conducted for goals that are neither political nor social. For example, the worst denial-of-service attacks have generally been conducted to extort money from victims, put competitors out of business, and satisfy the egos and curiosity of young hackers. Second, the attacks that have been linked to political and social goals have generally not been intimidating. Most

have been simple web defacements that, while annoying and disruptive, do not have much impact. They correspond more to the activity one might expect to see from protestors, not terrorists. For this reason, such cyber attacks are often referred to as "hacktivism," reflecting the convergence of hacking with activism rather than terrorism.

To fall in the domain of cyberterror, a cyber attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism, and it must be conducted for political and social reasons. Critical infrastructures, which include telecommunications, electrical power, oil and gas, water supply, transportation, banking and finance, emergency services, and essential government services, are likely targets. Attacks against these infrastructures that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or billion dollar banking losses would be examples.

To date, the most serious reported attack against a critical infrastructure took place in Australia in early 2000. A 49-year-old Brisbane man penetrated the Maroochy Shire Council's waste management system and used radio transmissions to alter pump station operations. A million litres of raw sewage spilled into public parks and creeks on Queensland's Sunshine Coast, killing marine life, turning the water black, and creating an unbearable stench. However, the man's goals were neither political nor social. He was a former employee of the company that had installed the system, and was angry about being rejected for a council job.[4]

Several computer viruses and worms have affected critical infrastructures. For example, the Slammer worm shut down emergency 911 systems, ATM machines, and at least one airline booking system. It disabled the safety monitoring system at a nuclear power plant for nearly 5 hours and affected several electrical and water utilities. Although the source of the worm was not confirmed, it did not appear to be tied to any terrorists or terrorist motives. The worm's code contained a reference to the Honkers Union of China, a major Chinese hacking group.

There have been numerous attacks against financial systems, including bank fraud and credit card fraud. However, such attacks have been conducted for money, not to coerce governments and societies. A terrorist group could attempt to steal billions through a cyber attack, with the dual goals of getting money to fund their organization and of coercing a target government. So far, however, this has not happened.

Because there have been no incidents that are generally regarded as cyberterrorism, the term itself has come to raise eyebrows. Skeptics wonder if it is all hype, used mainly to justify spending on new programs and increased government surveillance of the Internet.

Besides bearing little relation to any actual cyber incidents, the term also fails to capture the bulk of what terrorists are doing in cyberspace. Terrorists are making extensive use of cyberspace to facilitate their objectives, and it is important to understand, exploit, and counter this use. Too much emphasis on cyberterror, especially if it is not a serious threat, could detract from other counter-terrorist efforts in the cyber domain.

NPS/CTIW Studies

The first comprehensive treatment of the cyberterrorism threat was performed by the Center on Terrorism and Irregular Warfare (CTIW) at the Naval Postgraduate School (NPS) in Monterey, California. In August 1999, they issued a report on the prospects of terrorist organizations pursuing cyberterrorism.[5] They concluded that the barrier to entry for anything beyond annoying hacks is quite high, and that terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation. Cyberterrorism, they argued, was a thing of the future, although it might be pursued as an ancillary tool.

The NPS study defined three levels of cyberterror capability:

- *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 attacks capable of 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.

They estimated that it would take a group starting from scratch 2-4 years to reach the advanced-structured level and 6-10 years to reach the complex-coordinated level, although some groups might get there in just a few years or turn to outsourcing or sponsorship to extend their capability.

The study examined five terrorist group types: religious, New Age, ethno-nationalist separatist, revolutionary, and far-right extremists. They determined that only the religious groups are likely to seek the most damaging capability level, as it is consistent with their indiscriminate application of violence. New Age or single issue terrorists, such as the Animal Liberation Front, pose the most immediate threat, however, such groups are likely to accept disruption as a substitute for destruction. Both the revolutionary and ethno-nationalist separatists are likely to seek an advanced-structured capability. The far-right extremists are likely to settle for a simple-unstructured capability, as cyberterror offers neither the intimacy nor cathartic effects that are central to the psychology of far-right terror. The study also determined that hacker groups are psychologically and organizationally ill-suited to cyberterrorism, and that it would be against their interests to cause mass disruption of the information infrastructure.

In October 2000, the CTIW at NPS issued a second report following a conference aimed at examining the decision making process that leads sub-state groups engaged in armed resistance to develop new operational methods.[6] They were particularly interested in learning whether such groups would engage in cyber terrorism. In addition to academics and a member of the United Nations, the participants included a hacker and five practitioners with experience in violent sub-state groups. The latter included the PLO, the Liberation Tigers of Tamil Eelan (LTTE), the Basque Fatherland and Liberty-Political/Military (ETA-PM), and the Revolutionary Armed Forces of Colombia (FARC). The participants engaged in a simulation exercise based on the situation in Chechnya.

The "terrorist" team authorized only one cyber attack during the game, and that was against the Russian Stock Exchange. The attack was justified on the grounds that the exchange was an elite activity and thus disrupting it would not affect most Russians. Indeed, it might appeal to the average Russian. The group ruled out mass disruptions impacting e-commerce as being too indiscriminate and risking a backlash.

The findings from the meeting were generally consistent with the earlier study. Recognizing that their conclusions were based on a small sample, they concluded that terrorists have not yet integrated information technology into their strategy and tactics; that sub-state groups may find cyber terror attractive as a non-lethal weapon; that significant barriers between hackers and terrorists may prevent their integration into one group; and that politically motivated terrorists had reasons to target selectively and limit the effects of their operations, although they might find themselves in a situation where a mass casualty attack was a rational choice.

Cyberterror Indicators

The NPS researchers applied their general knowledge of terrorists and cyber weapons to evaluate the threat of cyberterrorism. By contrast, my recent work is based on identifying indicators of cyberterrorism. These are pieces of evidence that demonstrate a capability or intent to conduct acts of cyberterror. The ones I have identified so far fall into five categories:

- *Execution of cyber attacks*. This covers all types of computer network attack, not just acts of cyberterror.

- *Cyber weapons acquisition, development, and training*. This includes acquisition and distribution of cyber weapons, research and development in cyberweapons, and training in the use of cyberweapons. Activities can take place on-line or in special facilities.

- *Statements about cyber attacks*. This covers all types of statements relating to cyber attacks, including discussions, declarations of intent, and calls for performing cyber attacks.

- *Formal education in information technology*. This includes all areas of IT education, but especially studies in network and information security.

- *General experience with cyberspace*. This covers cyber activities that do not fall within the first four categories, including general use of the Internet for communications and distribution of news and propaganda.

The categories are listed in order of generally decreasing significance; that is, the actual execution of cyber attacks carries more weight than acquisition and development of cyber attack tools, which in turn carries more weight than simply making statements about cyber attacks, and so on. However, the ordering is not strict, as the nature of the evidence also matters. Evidence of a cyber training camp that has been instructing scores of cyber jihadists in attacks against the Supervisory Control and Data Acquisition (SCADA) would be a stronger indicator of cyberterrorism than evidence of a successful web defacement. SCADA and other types of digital control systems are used to monitor and control critical infrastructures such as for electricity, oil and gas, water, dams, and sewage, and are considered likely candidates for cyberterrorist attacks.

The last two categories, formal education in information technology (IT) and general experience in cyberspace are not indicators of cyberterrorism so much as enablers. A terrorist could study computer science, for example, in order to manage information resources such as websites for the organization. Even a focus on network security could be for the purpose of defending terrorist systems and information rather than launching cyber attacks. Still, terrorists with formal education in IT and experience using the technology are in a better position to develop a cyberterror capability than those without this background, so evidence in these categories is relevant to assessing the cyberterror threat.

In seeking evidence relating to these indicators, I considered activities attributable not only to terrorist groups, but also to hackers expressing an alliance or sympathies with such groups. Although the latter may not be willing to engage in physical acts of violence, they may be amenable to causing extensive damage to information resources. Also, it can be difficult to know the exact relationship between a terrorist group and hackers claiming some sort of affiliation. The Al-Qaeda Alliance Online, for example, appeared to have no formal ties to the terrorist organization, but it might be considered part of the broader jihadi movement associated with it.

The following subsections discuss each of the five indicator categories and the evidence I have found so far.

Execution of Cyber Attacks

Evidence of successful or even attempted computer network attacks is generally the strongest indicator of a cyberterrorism threat. However, as suggested above, the specifics involved in such attacks also matter, including the objectives, targets, results, methods, and overall prevalence. Attacks that seek to cause harm and generate fear are a stronger

indicator of cyberterrorism than ones that seek only other types of objectives such as money. Even if terrorists fund their operations by hacking web servers and stealing credit card numbers, for example, such attacks would fall more in the domain of terrorist support operations than acts of terrorism.

In addition, attacks against critical infrastructures are a stronger indicator than those against websites and non-essential services. Whether an attack is successful and the level of damage it causes also matters. Even so, a failed attack against the power grid would be more indicative of a cyberterror threat than a successful web defacement. The level of skill involved in an attack, as displayed through the methods used, is another important factor in judging an attack's significance. Finally, a single, isolated attack bears less significance than a demonstrated capability manifest in multiple attacks.

Over the years, numerous cyber attacks have been attributed to hackers affiliated with terrorist organizations or sympathetic to terrorist causes. Although none of these attacks has caused sufficient damage to be labeled an act of cyberterror, they have demonstrated a capability to disrupt e-mail and web services, and to use cyber attacks to raise money.

The first reported incident of this nature took place in 1997 when an offshoot of the Liberation Tigers of Tamil Eelam (LTTE) claimed responsibility for "suicide email bombings" against Sri Lankan embassies over a two-week period. Calling themselves the Internet Black Tigers, the group swamped Sri Lankan embassies with about 800 emails a day. The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications."[7] The Tamil Tigers are also credited with using a cyber attack to raise money. After compromising a computer system at Sheffield University in England in 1997 and capturing the user IDs and passwords of respected faculty, they used the email accounts to send out messages asking donors to send money to a charity in Sri Lanka.[8]

The Kosovo conflict in 1999 inspired numerous hackers to join the conflict on one side or the other, or to protest the whole thing. Most of their cyber attacks took the form of web defacements, but there were also a few denial of service attacks. Of particular interest here are the activities of the Serb Black Hand (Crna Ruka) group, because of the radical nature of Crna Ruka. According to reports, they crashed a Kosovo Albanian web site, justifying their actions with the statement "We shall continue to remove ethnic Albanian lies from the Internet." They also planned daily actions against NATO computers and deleted data on a Navy computer.[9]

Several years ago, the Animal Liberation Front took responsibility for a few cyber attacks. These included web defacements and virtual sit-ins (modest denial of service attacks against websites). They threatened additional cyber attacks, but I have not seen evidence of such.

The Israeli-Palestinian conflict has provoked numerous cyber attacks from hackers on both sides of the conflict. This was especially intense during the Second Intifada, which erupted in late September 2000. According to the security firm iDefense, at least two of

the pro-Palestinian groups involved in the parallel cyber intifada had terrorist connections.[10] One of these was UNITY, a Muslim extremist group with ties to Hizballah. After pro-Israeli hackers attacked Hizballah's website, the hackers launched a coordinated, multi-phased denial of service attack, first against official Israeli government sites, second against Israeli financial sites, third against Israeli ISPs, and fourth, against "Zionist E-Commerce" sites. The other group, al-Muhajiroun, has ties to a number of Muslim terrorist organizations as well as bin Laden. The London-based group directed their members to a Web page, where at the click of a mouse members could join an automated flooding attack against Israeli sites that were attacking Moqawama (Islamic Resistance) sites. iDefense also noted that UNITY recruited and organized a third group, Iron Guard, which conducted more technically sophisticated attacks. According to a Canadian government report, the group's call for cyber jihad was supported and promoted by al-Muhajiroun.[11]

The opening paragraph of this paper mentions the cyber attacks by GForce Pakistan and the formation of the Al-Qaeda Alliance Online in the wake of the September 11 attacks. Muslim hackers associated with one of the other Alliance members, the Pakistan Hackerz Club (PHC), had already defaced numerous websites with messages supporting Kashmir independence and the Palestinians. During the cyber intifada in November 2000, Doctor Nuker, a founder of PHC, posted 700 credit card numbers and 3,500 e-mail addresses on the website of the American Israel Public Affairs Committee. He had acquired the data from the web server when he broke into it.

In 2003, a call for cyber attacks against Israeli computers appeared on a website affiliated with Al-Qassam Brigades, the military wing of Hamas. Under the heading "the electronic jihad," someone opened a discussion about using computer viruses to inflict harm on Israel. The idea was to load a virus-infected page onto a website and then take steps to attract as many Israeli visitors as possible to the site.[12]

In early 2004, Internet Haganah, a website devoted to confronting Islamic terrorists on the Internet and stopping their use of the net as a communications and propagation tool, reported that the Al Aqsa Martyrs Brigade was planning a cyber attack against the El Al website.[13] Internet Haganah also reported that its own website, which is part of the Israeli domain ".il," was the target of jihadists. A message posted to a Yahoo! group attempted to recruit 600 Muslims for jihad cyber attacks against Internet Haganah. The motive was retaliation against Internet Haganah's efforts to close down terrorist-related websites. Muslim hackers were asked to register to a Yahoo! group called Jehad-Op.[14]

According to the Anti-Terrorism Coalition (ATC), the jihad was organized by a group named Osama Bin Laden (OBL) Crew, which also threatened attacks against the ATC website.[15] Founded in 2000 by an al-Qa'ida member living in Holland, since 2002 OBL Crew has been under the leadership of a San Diego man calling himself Ibn Shahbaz. Although the promised attacks against ATC either failed or never materialized, OBL Crew hackers did take over the Asian Hangout forum on June 26, 2004, which they used for recruiting.

As I complete this article in February 2006, Zone-h has recorded over two thousand web defacements, many in Denmark, protesting the twelve cartoons satirizing the Prophet Mohammad that were first published in the Danish newspaper *Jyllands-Posten*. While many of the attacks were conducted "just for fun," "as a challenge," and "to be the best defacer," the substantial number performed for "political reasons," "patriotism," and "revenge" might be indicative of a growing cadre of cyber jihadists. According to Zone-h, one of the defacers, the Internet Islamic Brigades (IIB), had also posted warnings of suicide bombings on a Danish forum, suggesting the group was interested in more than just relatively minor cyber attacks.[16]

According to the Jamestown Foundation, the radical jihadist al-Ghorabaa website coordinated a 24-hour cyber attack against *Jyllands-Posten* and other newspapers sites. Participants in the al-Ghorabaa forum also discussed broadening their campaign. Following the burning of the Danish and Norwegian embassies in Damascus and Beirut, they purportedly called for a global "embassy-burning day" against Danish embassies all over the world.[17] Internet Haganah also reported that a group (perhaps the same?) claiming credit for attacking Jyllands-Posten's website had released a video purporting to document the attack. The video was in the style of jihadi videos coming out of Iraq, showing that the hackers were emulating the tactics of violent jihadists.[18] These activities show an association between hacking and more violent forms of jihad, which could be precursors to cyberterrorism.

Cyber jihadists have also conducted cyber attacks in support of other objectives, including intelligence collection and information sharing. In an article on the challenges of terrorism in the information age, Magnus Ranstorp reports that al-Qa'ida had broken into the e-mail account of a U.S. diplomat in the Arab world. The terrorists had used simple password cracking tools, freely available on the Internet, to gain access to the account. They had retrieved his bank statements, which revealed information about his location and movement.[19]

Terrorists or their sympathizers have reportedly hijacked Internet servers in order to share documents. While this might not be considered an "attack," it nonetheless represents unauthorized use of computers. In one such case, 70 files were uploaded to an unprotected File Transfer Protocol (FTP) site run by the Arkansas government for its contractors. A person calling himself Irhabi 007, or Terrorist 007, put links to the files on a message board belonging to al Ansar.[20] The motivations for using hijacked sites could include access to free storage and avoidance of detection by authorities.

Cyber Weapons Acquisition, Development, and Training

Terrorist groups typically supply their members with weapons, acquired on black markets or developed in-house. They also provide training in the use of these weapons. Al-Qa'ida, for example, operated training camps in Afghanistan and Sudan for thousands of jihadists. Some of these facilities are also used for weapons research and development. In addition, terrorists provide training materials in the form of written documents and

videos, which are distributed to members. One video even shows how to build a suicide belt.

If terrorists are to conduct highly damaging cyber attacks, I would expect to see similar activities in the cyber domain, including acquisition, research, development, distribution, and training in cyber weapons. So far, there have been a few such indicators. According to Magnus Ranstorp, an al-Qa'ida safe house in Pakistan was used to train operational members in computer hacking and to conduct cyber reconnaissance against infrastructure and SCADA systems, probing the control mechanisms of electrical power grids and dam structures.[21] While this could be a strong indicator of an attempt to develop a cyberterror capability, I could not find any other information about it or information suggesting that al-Qa'ida had developed or acquired cyber tools for attacking these systems.

In January 2002, the National Infrastructure Protection System (NIPC) also reported that al-Qa'ida members had "sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related websites. They specifically sought information on water supply and wastewater management practices in the U.S. and abroad." The NIPC bulletin also noted that the FBI had found structural architecture software (CATIGE, BEAM, AUTOCAD 2000, and MICROSTRAN) on the computer of a person with indirect ties to bin Laden. The software suggested the individual was interested in structural engineering as it relates to dams and other water-retaining structures.[22] However, the software could be useful in planning either physical or cyber attacks against these structures, so the research is not necessarily related to cyberterror.

Other indicators point to on-line training in cyber attacks. In late 2003, an affiliate of al-Qa'ida announced the opening of Al-Qa'ida University for Jihad Sciences on the Internet, with a college on electronic jihad. The announcement was circulated by the Islamic Information Center, which in the past had disseminated statements by bin Laden on the Internet. The other colleges include the technology of explosive devices, booby-trapped cars and vehicles, and media jihad. The announcement noted that there were already specialists in electronic Jihad.[23]

In August 2005, the Jamestown Foundation reported that the jihadist al-Farouq web forum contained postings calling for heightened electronic attacks against U.S. and allied government websites, and information for mujahid hackers. The website included a hacker library with information for disrupting and destroying enemy electronic resources. The library held keylogging software for capturing keystrokes and acquiring passwords on compromised computers, software tools for hiding or misrepresenting the hacker's Internet address, and disk and system utilities for erasing hard disks and incapacitating Windows-based systems.[24]

Two months later, Jamestown reported that a manual on hacking was posted on another Internet forum frequented by jihadists, Minbar ahl al-Sunna wal-Jama'a (The Pulpit of the People of the Sunna). The document was said to be written in a pedagogical style and discuss motives and incentives for computer-based attacks, including political, strategic,

economic, and individual. It was also said to discuss three types of attack: direct intrusions into corporate and government networks, infiltration of personal computers to steal personal information, and interception of sensitive information such as credit card numbers in transit.[25]

In February 2006, Jamestown noted that "Most radical jihadi forums devote an entire section to [hacker warfare]." They said that the al-Ghorabaa site, which had coordinated an attack against *Jyllands-Posten*, contained information on penetrating computer devices and intranet servers, stealing passwords, and security. It also contained an encyclopedia on hacking sites and a 344-page book on hacking techniques, including a step-by-step guide for "terminating pornographic sites and those intended for the Jews and their supporters."[26]

Imam Samudra, one of the terrorists convicted in the October 12, 2002 Bali bombings, offers rudimentary information on hacking, particularly as it applies to credit card fraud ("carding") in a chapter titled "Hacking: why not?" of his autobiography *Me Against the Terrorist!* Sumadra advocates the use of computer attacks to raise funds for terrorist activities. Evidence found on his seized computer showed he at least had made an attempt at carding.[27]

Hacking groups provide a forum for exchanging cyber attack tools and methods, and learning how to use them. Although much of the activity takes place online, in some cases, members meet in person and learn from each other. In 1998, for example, the Muslim Hackers Club (MHC) sent an e-mail announcing that their president, brother Ibrahim, would be visiting Pakistan and offering local MHC chapters classes in hacking Internet Service Providers and network protocols. The classes would also teach how to set up Windows-NT-based servers. The message went on to say that "MHC's main orientation will be to setup a nonstate capability in information warfare, err, research, if that makes you feel better." The MHC also operated a website with hacking information, tutorials, and software tools.[28]

There are thousands of hacking groups worldwide. A group could align itself with terrorists at any time, adding to the skill base that can be applied to cyberterrorism. Even though the overwhelming majority would never support terrorism, evidence has shown that at least some have hacked in support of the same objectives.

Statements About Cyber Attacks

Statements by terrorists pertaining to the use cyber attacks can indicate an interest or intent to carry out cyberterrorism. Such statements can take the form of exploratory discussions, forecasts, threats, advocacy, calls to action, and claims relating to capability or responsibility for attacks.

In some cases, statements about cyberterrorism have been issued in conjunction with lesser attacks. For example, not long after September 11, an anti-US defacement carried the message: "IN NEXT DAYS YOU'LL LOOK THE GREATEST

CYBERTERRORIST ATTACK AGAINST AMERICAN GOVERNMENT COMPUTERS." The threatened cyberterrorism, however, never materialized.

Various statements from al-Qa'ida and its supporters have shown that the possibilities of cyberterrorism are at least on the terrorist network's radar screen. For example, following the September 11 attacks, Osama bin Laden allegedly told Hadmid Mir, editor of the *Ausaf* newspaper, that "hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and (sic) ranging from computers to electronics against the infidels."[29]

In December 2001, *Newsbytes* reported that a suspected member of al-Qa'ida said that members of the terrorist network had infiltrated Microsoft and attempted to plant Trojan horses and bugs in the Windows XP operating system.[30] According to the report, Mohammad Afroze Abdul Razzak told Indian police that the terrorists had gained employment at Microsoft by posing as computer programmers. Microsoft responded by saying the claims were "bizarre and unsubstantiated and should be treated skeptically." Although the claims are almost certainly false, the story is troubling for the simple reason that it shows that at least some terrorists are fully cognizant of the potential of cyber attacks and how such attacks can be launched with the aid of Trojan horses and insider access into the world's dominant software producer.

National Review reported that a Syrian cyberterrorist whose day job was running a car dealership invited potential Islamic hackers to join the Arab Electronic Jihad Team (AEJT). Announced in 2002, the goals of AEJT were to bring down all websites in the United States and Israel. The group sought members who were "advanced in the art of hacking."[31] As 2002 drew to a close, U.S. and Israeli websites remained standing.

Sheikh Omar Bakri Muhammad, the London-based Islamic cleric who heads al-Muhajiroun and has ties to bin Laden, told *Computer World* in November 2002 that al-Qa'ida and other radical Muslim groups were actively planning to use the Internet as a weapon in their holy war against the West. He noted that the military wings of al-Qa'ida and other radical Islamic groups were using and studying the Internet for their own operations. He said that "in a matter of time, you will see attacks on the stock market," and that he "would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."[32]

As noted earlier, postings on the al-Farouq website in 2005 called for cyber attacks against the U.S. and allied governments. One participant, who identified himself as "archrafe," proposed forming an operations unit within the Islamic Hacker Army (Jaish al-Hacker al-Islami). He offered advantages to organizing the electronic jihad community, including the ability to launch simultaneous denial of service attacks.[33]

Two years earlier, a book advocating cyber attacks against infidel websites was posted on al-Farouq's website. Titled *The 39 Principles of Jihad*, the book calls upon every Muslim to "obey the Jihad against the infidels." The principles suggest different ways of doing so, including participating in martyrdom and other operations, supplying money

and equipment to fighters, and so forth. Principle 34 specifically directs computer experts to "use their skills and experience in destroying American, Jewish and secular websites as well as morally corrupt web sites."[34]

According to Fouad Husseing, cyberterrorism is part of al-Qa'ida's long-term war against the U.S. In his book, *al-Zarqawi-al-Qaeda's Second Generation*, Husseing describes al-Qa'ida's seven-phase war as revealed through interviews of the organization's top lieutenants. Phase 4, which is scheduled for the period 2010-2013, includes conducting cyberterrorism against the U.S. economy.[35] Given other evidence, this is conceivable.

Formal Education in Information Technology

Although it is not hard to carry out relatively simple cyber attacks using readily available hacking tools, considerably greater skill would be required to develop software to perform original and highly damaging attacks against critical infrastructures. For such attacks, formal education in a field such as computer science or computer engineering would be helpful, especially if the program of study included digital controls sytems and network security. Although courses in information and network security emphasize how to defend against cyber attacks, they inevitably teach something about attacks, as it is not possible to build adequate defenses without a solid understanding of the threat.

A few people with formal education in these areas have been associated with terrorist groups. Sami Al-Arian, the professor at the University of South Florida charged with raising money for Palestinian Islamic Jihad, was in the department of Computer Science and Engineering. Although Al-Arian's area of specialty did not appear to be network security, Sami Omar Al-Hussayen, the Saudi graduate student at the University of Idaho charged with operating websites used to recruit terrorists, raise money to support terrorism, and disseminate inflammatory rhetoric, was studying computer security in the Computer Science Department. However, neither Al-Arian or Al-Hussayen were convicted of any crimes.

In *Black Ice*, Dan Verton describes how a computer science major at Columbia College in Missouri became al-Qa'ida's procurement officer in the U.S. for computers, satellite telephones, and sophisticated surveillance technologies. Along the way, Ziyad Khalil, using the pseudoname Ziyad Sadaqa, registered as the operator of Hamas's website, www.palestine-info.net. From there, he eventually came to the attention of al-Qa'ida.[36]

In perhaps the most significant case of all, a computer science graduate student at Bradley University was allegedly assigned by al-Qa'ida to explore ways of hacking into the computer systems of U.S. banks and to help settle al-Qa'ida members entering the United States for attacks. According to reports, Ali S. Marri had been trained in computer hacking and the use of poisons, and had met Osama bin Laden at the al Farooq camp in Afghanistan. Marri was designated an enemy combatant by President Bush in 2003.[37] This is the only case where the subject's activities and educational program were tied to an objective of conducting cyber attacks. Those of Al-Arian, Al-Hussayen, and Khalil did not appear to involve cyber attacks.

General Experience With Cyberspace

Although most people who use computers and the Internet never conduct any cyber attack, it is also true that experience with the technology is a prerequisite for conducting destructive cyber attacks. Terrorist groups that make extensive use of cyberspace are better equipped to move in the direction of employing cyberterrorism than those that do not.

In this regard, numerous terrorist groups, and especially those affiliated with al-Qa'ida and the global jihad, have made extensive use of cyberspace to distribute documents, videos, audio recordings, and other materials; and to communicate with cohorts, recruit, raise money, gather intelligence about targets and weapons, discuss options, and generally facilitate their organizations and operations. They have operated websites with password-protected areas and used e-mail, web forums and discussion groups, instant messaging and chat, and encryption.[38,39,40] Jihadists are even said to have developed a web browser that filters out all websites except for that of the pre-eminent Salafist ideologue Abu Muhammad al-Maqdisi.[41] However, none of these activities require the skills needed to carry out cyber attacks, so they are not strong indicators of cyberterror.

Conclusions

The foregoing evidence shows that terrorist groups and jihadists have an interest in conducting cyber attacks and at least some capability to do so. Further, they are attempting to develop and deploy this capability through online training and calls for action. The evidence does not, however, support an imminent threat of cyberterrorism. Any cyber attacks originating with terrorists or cyber jihadists in the near future are likely to be conducted either to raise money (e.g., via credit card theft) or to cause damage comparable to that which takes place daily from web defacements, viruses and worms, and denial-of-service attacks. While the impact of those attacks can be serious, they are generally not regarded as acts of terrorism. Terrorists have not yet demonstrated that they have the knowledge and skills to conduct highly damaging attacks against critical infrastructures (e.g., causing power outages), although there are a few indicators showing at least some interest. Using the terminology from the 1999 NPS study, their capability is at the lowest level, namely that required to carry out simple-unstructured attacks.

A disclaimer, however, is in order. The assessment is based entirely on open sources. Intelligence agencies may have addition information that would suggest a higher level of threat. Further, terrorists could be engaging in cyber activities that have not even made the radar screens of the intelligence agencies.

Looking further into the future, it is difficult to know where terrorism might lead. It is conceivable that cyber weapons will never draw the appeal of bombs and other physical weapons. However, I can suggest a few indicators that would likely precede a successful incident of cyberterror:

- Failed cyber attacks against critical infrastructures, particularly the SCADA and other digital systems that are used to monitor and control these infrastructures. It seems unlikely that a first attempt would succeed with the desired effect, given the novelty of such an attack and uncertainty about how it would play out.

- Research and training labs, where terrorists simulate the effects of cyber attacks against critical infrastructures, develop methods and tools of attack against those infrastructures, and train people on how to conduct such attacks. Although hackers use the Internet itself as their research and training lab, trying out various attacks on live systems, it is hard to perform controlled experiments and analyze the consequences without a lab. Absent special facilities, I would expect to at least see training materials showing terrorists how to conduct damaging attacks against critical infrastructures and software tools designed to facilitate such attacks.

- Extensive discussions and planning relating to acts of cyberterror against critical infrastructures, not just attacks against websites and attacks aimed at making money.

Many authors have suggested that terrorists may be more inclined to use cyberterror as an ancillary tool to amplify the effects of a physical attack. For example, they might launch a cyber attack against the emergency 911 system while blowing up a hotel, the goal being to impede response to the incident and increase fear. However, terrorists do not normally integrate multiple modes of attack. While there have been numerous incidents involving coordinated attacks – including the 9/11 hijackings, the London subway bombings, the Madrid train bombings, and the East African Embassy bombings – these have always involved multiple occurrences of pretty much the same thing (e.g., 4 hijacked planes turned into missiles in the 9/11 attacks). It seems unlikely that terrorists would suddenly succeed with an attack requiring coordination across the cyber and physical domains. Even if this becomes their goal, I would expect to see evidence of failed attempts, cross-domain training and simulation, and discussions and planning relating to such attacks before a successful incident. Given terrorists' capabilities today in the cyber domain, this seems no more imminent than other acts of cyberterror.

In summary, my overall assessment of the cyberterror threat is much the same as five years ago. At least in the near future, bombs remain a much larger threat than bytes. However, we cannot ignore the potential of cyberterror. During the past five years, terrorists and jihadists have shown a stronger interest in and capability to conduct cyber attacks, and they have successfully conducted numerous attacks against websites.

Moreover, even if our critical infrastructures are not under imminent threat by terrorists seeking political and social objectives, they must be protected from harmful attacks conducted for other reasons such as money, revenge, youthful curiosity, and war. The owners of these infrastructures and their governments must defend against cyber attacks regardless of who may perpetrate them.

Endnotes

[1] Brian McWilliams, "Pakistani Hackers Deface U.S. Site With Ultimatum, *Newsbytes*, October 17, 2001.

[2] Dorothy E. Denning, "Cyberterrorism," Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000.

[3] Dorothy E. Denning, "Is Cyber Terror Next?" in *Understanding September,* Craig Calhoun, Paul Price, and Ashley Timmer, eds., The New Press, 2002; also placed on SSRC website November 2001.

[4] "Sewage Hacker Jailed," *Herald Sun,* October 31, 2001.

[5] Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell, and Greg Gagnon, "Cyberterror: Prospects and Implications," Center for the Study of Terrorism and Irregular Warfare, Monterey, CA, August 1999.

[6] David Tucker, "The Future of Armed Resistance: Cyberterror? Mass Destruction?" Conference Report and Proceedings, Center for the Study of Terrorism and Irregular Warfare, Monterey, CA, October 2000.

[7] "Email Attack on Sri Lanka Computers," *Computer Security Alert,* No. 183, Computer Security Institute, June 1998, p. 8.

[8] Michael Vatis, "Cyber Terrorism and Information Warfare: Government Perspectives," in *Cyber Terrorism and Information Warfare,* Yonah Alexander and Michael S. Swetnam, eds., Transnational Publishers, Inc., 2001.

[9] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism," in *Networks and Netwars,* John Arquilla and David Ronfelt, eds., RAND, 2001, p. 273.

[10] Israeli-Palestinian Cyber Conflict, iDefense Intelligence Services Report, January 3, 2000.

[11] "Al-Qaida Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Threat Analysis TAV01-001, Government of Canada, November 2, 2001.

[12] "Hamas Sympathizers Have a Plan for Computers – Maybe Yours!" Internet Haganah, accessed April 8, 2003.

[13] Internet Haganah website at http://haganah.org.il/haganah/index.html, accessed March 24, 2004.

[14] Jeremy Reynalds, "Internet 'Terrorist' Using Yahoo to Recruit 600 Muslims for Hack

Attack," *Mensnewsdaily.com*, February 28, 2004, http://www.mensnewsdaily.com/archive/r/reynalds/04/reynalds022804.htm, accessed June 12, 2006.

[15] "ATC's OBL Crew Investigation," July 1, 2004. The ATC disbanded on June 3, 2006, and the article no longer appears to be online.

[16] Roberto Preatoni, "Prophet Mohammed Protest Spreads on the Digital Ground," *Zone-h*, February 7, 2006, http://www.zone-h.org/content/view/10/30/, accessed June 12, 2006.

[17] Stephen Ulph, "Internet Mujahideen Refine Electronic Warfare Tactics," *Terrorism Focus*, Vol. III, Issue 5, Jamestown Foundation, February 7, 2006.

[18] "How the Brothers Attacked the Website of Jyllands-Posten," Internet Haganah, February 7, 2006, http://haganah.org.il/harchives/005456.html, accessed June 12, 2006.

[19] Magnus Ranstorp, "Al-Qaida in Cyberspace: Future Challenges of Terrorism in an Information Age," in *Terrorism in the Information Age – New Frontiers?*, Lars Nicander and Magnus Ranstorp, eds., Swedish National Defence College, 2004.

[20] David McGuire, "Al Qaeda Messages Posted on U.S. Server," *The Washington Post*, July 13, 2004.

[21] Magnus Ranstorp, "Al-Qaida in Cyberspace: Future Challenges of Terrorism in an Information Age," in *Terrorism in the Information Age – New Frontiers?*, Lars Nicander and Magnus Ranstorp, eds., Swedish National Defence College, 2004.

[22] National Infrastructure Protection Center, Terrorist Interest in Water Supply and SCADA Systems," Information Bulletin 01-001, January 30, 2002.

[23] "Al-Qa'ida Reportedly Establishing Open 'Internet University' to Recruit Terrorists," OSAC Foreign Press Report of article by Muhammad al-Shafi in London *Al-Sharq al-Awsat* in Arabic, November 20, 2003.

[24] Jeffrey Pool, "New Web Forum Postings Call for Intensified Electronic Jihad Against Government Websites," Jamestown Foundation, August 23, 2005.

[25] Jeffrey Pool, "Technology and Security Discussions on the Jihadist Forums," Jamestown Foundation, October 11, 2005.

[26] Stephen Ulph, "Internet Mujahideen Refine Electronic Warfare Tactics," *Terrorism Focus*, Vol. III, Issue 5, Jamestown Foundation, February 7, 2006.

[27] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace," *The Washington Post*, December 14, 2004, p. A19.

[28] "Computer Lessons for Terrorists," *Newsweek*, May 20, 2002.

[29] "Al-Qaida Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Threat Analysis TAV01-001, Government of Canada, November 2, 2001.

[30] Brian McWilliams, "Suspect Claims Al Qaeda Hacked Microsoft," *Newsbytes*, December 17, 2001.

[31] James S. Robbins, "The Jihad Online," *National Review Online*, July 30, 2002, http://nationalreview.com/robbins/robbins073002.asp, accessed June 12, 2006.

[32] Dan Verton, "Bin Laden Cohort Warns of Cyberattacks," *Computerworld*, November 18, 2002; Dan Verton, "Al-Qaeda Poses Threat to Net," *Computerworld*, November 25, 2002.

[33] Jeffrey Pool, "New Web Forum Postings Call for Intensified Electronic Jihad Against Government Websites," Jamestown Foundation, August 23, 2005.

[34] Jonathan D. Halevi, "39 Principles of Jihad," Center for Special Studies, Intelligence and Terrorism Information Center, September 2003, http://www.intelligence.org.il/eng/var/39p_e.htm, accessed June 12, 2006.

[35] Allan Hall, "Al-Qaeda Chiefs Reveal World Domination Design," *The Age*, August 24, 2005.

[36] Dan Verton, *Black Ice*, Mc-Graw Hill, 2003, pp. 88-91.

[37] Susan Schmidt, "Qatari Man Designated an Enemy Combatant," *Washington Post*, June 24, 2003, p. A01.

[38] Dorothy E. Denning, "Information Operations and Terrorism," to appear in *Innovative Terrorism in the Information Age: Understanding the Threat of Cyber-Warfare*, Lars Nicander and Magnus Ranstorp, eds., Hurst, 2006.

[39] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars : The Future of Terror, Crime, and Militancy*, John Arquilla and David Ronfeldt, eds., 2001, pp. 239-288.

[40] Gabriel Weimann, www.terror.net, United States Institute of Peace Special Report 116, March 2004.

[41] "Jihadist Web Browser," posted by Terrorism.com staff, Open Source Center, February 8, 2006, http://www.fbis.gov, accessed June 12, 2006.